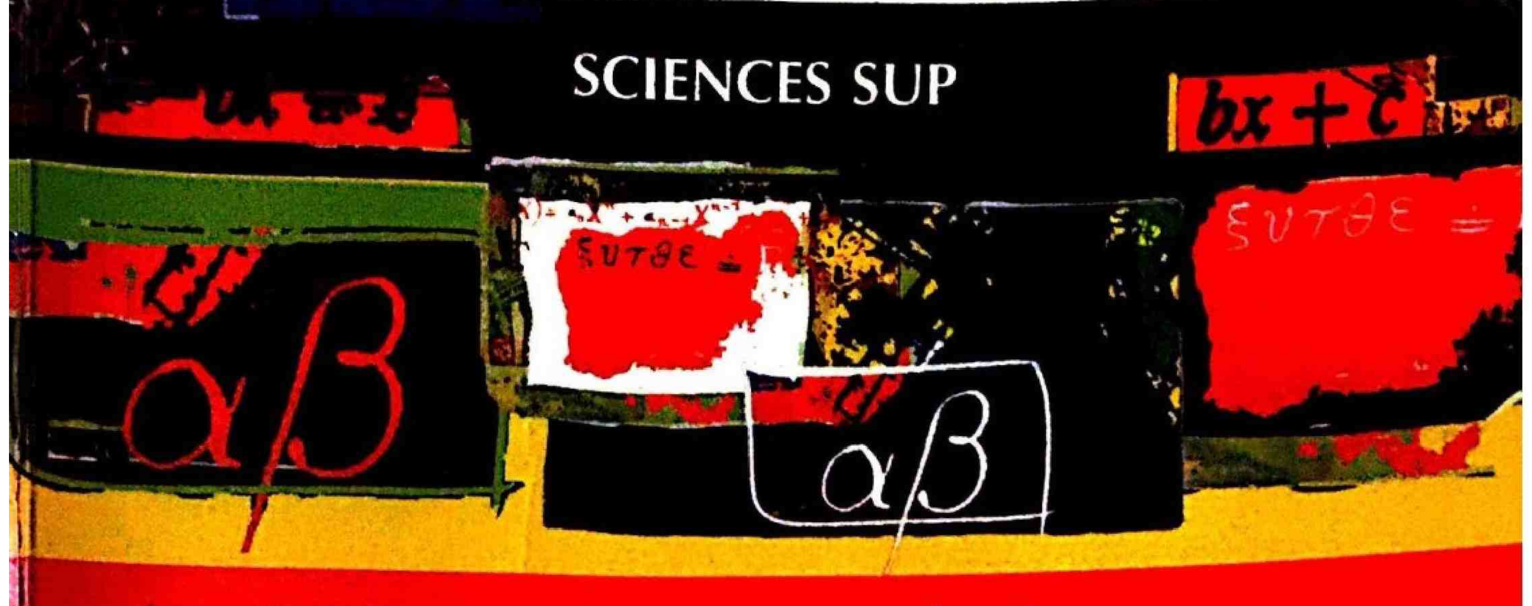



*Cours et exercices avec solutions*

**Licence 1re année MIAS • MASS • SM**

# ALGÈBRE 1re ANNÉE

2e édition

**François Liret**
**Dominique Martinais**



DUNOD

# ALGÈBRE

## 1re ANNÉE

## Cours et exercices avec solutions



***François Liret***
Maître de conférences
à l'université Paris 7 - Denis Diderot

***Dominique Martinais***
Maître de conférences
à l'université Paris 7 - Denis Diderot

Préfacé par
***Michel Zisman***
Professeur émérite de l'Université Paris 7 - Denis Diderot

**2e édition**

DUNOD

# Préface

Pourquoi publier un nouveau manuel ? Après tout, au cours des dix et même des vingt dernières années les programmes ont peu changé : tout au plus un chapitre un peu marginal se trouve-t-il parfois ajouté, parfois supprimé. Dans l'ensemble ce que doivent, ce que peuvent apprendre étudiantes et étudiants durant leurs deux premières années à l'université demeure à peu près stable.

Mais tout le reste est profondément modifié. La société d'aujourd'hui ne ressemble plus à celle d'hier, les lycées et leurs élèves ont changé, et aussi leurs professeurs. L'enseignement dans les universités lui non plus n'est pas resté figé.

Cette évolution, d'ailleurs preuve de vitalité, doit se traduire aussi dans les ouvrages proposés à celles et ceux qui abordent maintenant les études universitaires : le public d'aujourd'hui mérite des livres qui ont été écrits pour lui, par des auteurs qui ont suivi et qui ont compris son évolution.

Telle est l'ambition de cette collection de premier cycle de mathématiques confiée à François Liret et Dominique Martinais qui apporte à ses lecteurs non seulement une présentation impeccable plaisante à l'œil et donc facile à lire, mais surtout le fruit d'années d'expérience et de réflexion sur la manière de rédiger un texte scientifique, sur l'importance respective de la présentation des *outils* qu'ils devront apprendre à manier, des *démonstrations* qui sont l'âme des mathématiques et des *explications* indispensables à la compréhension de celles-ci. Le cours est illustré d'exemples et d'exercices judicieux, qui apporte aux lecteurs tout ce qui leur est nécessaire pour réussir pleinement leurs études.

**Michel Zisman**

Professeur émérite de l'université Paris 7 - Denis Diderot

# Table des matières

# Avant-Propos

Nous avons voulu que ce cours de première année reste élémentaire et que les résultats en soient démontrés soigneusement. L'exposé est en général très détaillé : nous espérons qu'il permettra aux étudiants d'apprendre à raisonner. Nous avons également tenu à présenter les algorithmes de calcul qu'il est nécessaire de pratiquer et à mettre en évidence des conseils pour chercher les exercices. Lorsque dans le texte, l'un des mots théorème, proposition ou corollaire est souligné, c'est qu'il s'agit d'un énoncé important.

Puisse ce manuel aider les étudiants dans leur apprentissage des mathématiques.

Nous devons un grand merci à Michel Zisman qui nous a patiemment relus et dont les conseils et nombreuses suggestions nous ont été très utiles. Merci également à Alberto Arabia qui a mis son talent et sa compétence en informatique au service de la mise en page. Enfin nous remercions Anne Bourguignon qui s'est chargée avec efficacité de l'édition de ce livre.

Les auteurs

Cette présente édition est l'occasion de préciser ou de simplifier le cours et d'y ajouter commentaires, exemples et exercices traités. De nouveaux exercices d'entraînement, avec indications de solutions, sont aussi proposés. En arithmétique, nous avons introduit la fonction indicatrice d'Euler et en analyse, la notion de longueur d'un arc paramétré.

Plusieurs collègues et amis nous ont suggéré des améliorations et permis de corriger des fautes, nous les remercions vivement.

# Principales notations utilisées

## Quelques lettres grecques employées en mathématiques

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $\alpha$ | alpha | $\varepsilon$ | epsilon | $\lambda, \Lambda$ | lambda | $\sigma, \Sigma$ | sigma |
| $\beta$ | bêta | $\zeta$ | zêta | $\mu$ | mu | $\varphi, \Phi$ | phi |
| $\gamma, \Gamma$ | gamma | $\eta$ | êta | $\pi, \Pi$ | pi | $\psi, \Psi$ | psi |
| $\delta, \Delta$ | delta | $\theta$ | thêta | $\rho$ | rho | $\omega, \Omega$ | oméga |

## Principales notations utilisées

| | |
|---|---|
| $\mathbb{N}$ | ensemble des entiers naturels |
| $\mathbb{Z}$ | anneau des entiers relatifs |
| $\mathbb{Q}$ | corps des nombres rationnels |
| $\mathbb{R}$ | corps des nombres réels |
| $\mathbb{C}$ | corps des nombres complexes |
| $E \setminus A$ | complémentaire de la partie $A$ dans l'ensemble $E$ |
| $E \times F$ | produit cartésien des ensembles $E$ et $F$ |
| $f : A \to B$ | application d'un ensemble $A$ dans un ensemble $B$ |
| $f^{-1}$ | bijection réciproque de la bijection $f$ |
| $\mathrm{id}_E$ | application identique de l'ensemble $E$ |
| $\mathrm{Card}\, A$ | cardinal de l'ensemble fini $A$ |
| $C_n^p$ | nombre de parties à $p$ éléments d'un ensemble à $n$ éléments |
| $\mathcal{R}e\, z$, $\mathcal{I}m\, z$ | partie réelle, partie imaginaire du nombre complexe $z$ |
| $\|z\|$, $\mathrm{Arg}\, z$ | module, argument du nombre complexe $z$ |
| $\mathrm{pgcd}(a, b)$ | plus grand commun diviseur de $a$ et $b$ |
| $\mathrm{ppcm}(a, b)$ | plus petit commun multiple de $a$ et $b$ |
| $a \equiv b\ [n]$ | $a$ est congru à $b$ modulo $n$ |
| $\mathbf{K}$ | désigne $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ |
| $\mathbf{K}[X]$ | anneau des polynômes à coefficients dans $\mathbf{K}$ |
| $\deg P$ | degré du polynôme $P$ |
| $\mathbf{K}(X)$ | corps des fractions rationnelles à coefficients dans $\mathbf{K}$ |
| $M_{n,p}(\mathbf{K})$ | ensemble des matrices à $n$ lignes et $p$ colonnes à coefficients dans $\mathbf{K}$ |
| $M_n(\mathbf{K})$ | anneau des matrices carrées à $n$ lignes à coefficients dans $\mathbf{K}$ |
| $\mathrm{GL}_n(\mathbf{K})$ | groupe des matrices carrées inversibles à $n$ lignes à coefficients dans $\mathbf{K}$ |
| $\det A$ | déterminant de la matrice carrée $A$ |
| $\dim E$ | dimension de l'espace vectoriel $E$ |
| $\mathrm{Im}\, f$, $\mathrm{Ker}\, f$ | image, noyau de l'application linéaire $f$ |
| $\mathcal{S}_n$ | groupe symétrique |

# Chapitre 1

# S'exprimer en mathématiques

Sous leur apparente diversité, les expressions employées en mathématiques se classent en quelques types réservés à des situations logiques précises. Quant aux raisonnements mathématiques, même les plus complexes, ils consistent en un enchaînement de déductions obéissant à un petit nombre de règles.

## Les énoncés

La plupart des phrases que l'on rencontre dans un livre de mathématiques concernent des objets mathématiques. Les phrases qui ont pour but de définir de tels objets, ou bien d'en affirmer des propriétés, ou simplement de les introduire s'appellent des *énoncés*.

Voici des exemples d'énoncés. Nous convenons qu'un entier positif n'est pas nul.

**(1)** Le nombre $\frac{7^{11}-7}{11}$ est un entier positif.

**(2)** Soit $x$ un nombre réel strictement positif.

**(3)** Il existe un entier naturel plus grand que $2^{100}$.

**(4)** Posons $a = \int_0^1 e^{t^2} dt$.

**(5)** Si $n$ est un entier relatif, alors $16n^2 - 48n + 33$ est un entier positif.

**(6)** Si $x$ est un nombre réel, le plus grand des nombres $x$ et $-x$ s'appelle la valeur absolue de $x$.

**(7)** Notons $I$ l'intervalle $[0, 1]$.

**(8)** Si $n$ est un entier positif, alors $n$ est impair ou $n(n+2)(n+3)$ est multiple de 4.

**(9)** Pour tout nombre réel $x$ tel que $x^2 > 2$, on a $x > 1$.

**(10)** Si $x$ est un nombre réel, la valeur absolue de $x$ se note $|x|$.

Certains énoncés affirment une propriété : ce sont des *propositions*. Par exemple, (1), (3), (5), (8) et (9) sont des propositions.

Un énoncé comme (2) permet de se donner un objet mathématique, en l'introduisant en général par le mot « soit ».

L'énoncé (6) définit et nomme un nouvel objet (la valeur absolue d'un nombre réel). Dans un livre de mathématiques, un tel énoncé s'appelle une **définition**.

Enfin, il y a des énoncés, comme (4), (7) ou (10), qui indiquent simplement que l'on va désigner par un certain symbole un objet précédemment défini : ce sont des *notations*. Une notation est le plus souvent introduite par l'un des mots « **posons** » ou « **notons** ».

## Les propositions

Elles sont coordonnées par des conjonctions comme « **donc** », « **d'où** », « **par suite** », « **par conséquent** », « **car** », « **puisque** », « **si et seulement si** », ou par des expressions comme « **il s'ensuit** », « **on en déduit** », « **il vient** », « **on obtient** », ou simplement « **on a** », ou encore par l'expression « **si** $\ldots$, **alors** $\ldots$ ».

Certaines propositions sont des expressions mathématiques écrites sous forme purement symbolique, comme par exemple $\sqrt{6} < 5/2$, ou encore $\int_0^\pi \sin t\, dt = 2$. Ces propositions n'étant pas des phrases, on doit les employer en utilisant des formes grammaticales correctes, notamment en ce qui concerne les verbes. Par exemple, il convient d'écrire « puisqu'on a $6 < 25/4$, on en déduit $\sqrt{6} < 5/2$ » et non pas « $\sqrt{6} < 5/2$ car $6 < 25/4$ ». Cependant, pour ne pas alourdir le style, des libertés sont permises, à la condition expresse qu'elles ne nuisent pas au sens. L'expression « on a $\sqrt{6} < 5/2$ car $6 < 25/4$ » est ainsi permise, bien qu'elle soit incorrecte selon les règles de la grammaire française.

> Une proposition est soit vraie, soit fausse et elle ne peut être à la fois vraie et fausse.

La proposition (1) est vraie, ainsi que (3). La proposition (5), du type « si $\ldots$, alors $\ldots$ », est constituée de deux propositions. La première est la proposition $P$ : « $n$ est un entier relatif » et la seconde est la proposition $Q$ : « $16n^2 - 48n + 33$ est un entier positif ». La proposition « si $P$, alors $Q$ » affirme que si $P$ est vraie, alors $Q$ est vraie également. Cette proposition (5) est vraie, de même que la proposition (8) qui est du même type. La proposition (9) a également la structure « si $\ldots$, alors $\ldots$ », car elle pourrait aussi bien se formuler sous la forme « si $x$ est un nombre réel tel que $x^2 > 2$, alors on a $x > 1$ ». Cette proposition (9) est fausse : en effet, $-2$ est un nombre réel, $(-2)^2$ est strictement plus grand que 2 et $-2$ n'est pas strictement plus grand que 1.



Voici les opérations que l'on peut effectuer avec des propositions.

**La négation.** Affirmer que la proposition $P$ : « $\sqrt{2}$ n'est pas un entier naturel » est vraie, c'est exprimer que la proposition $Q$ : « $\sqrt{2}$ est un entier naturel » n'est pas vraie, c'est-à-dire que la proposition $Q$ est fausse. On dit que $P$ est la négation de $Q$, ce qui se note $P = \text{non}(Q)$.

De manière générale, si $P$ est une proposition, alors une et une seule des propositions $P$ ou $\text{non}(P)$ est vraie et l'autre est fausse. Par suite, les propositions $P$ et $\text{non}(\text{non}(P))$ sont toutes les deux vraies ou bien toutes les deux fausses.

**L'opération « ou ».** Soit la proposition suivante, où $n$ et $p$ sont des entiers relatifs :

$R$ : « $np$ est pair ou $n^2 - p^2$ est multiple de 8 ».

Cette proposition est du type ($P$ ou $Q$), où $P$ est la proposition « $np$ est pair » et où $Q$ est la proposition « $n^2 - p^2$ est multiple de 8 ».

Par définition, une proposition de la forme ($P$ ou $Q$) est vraie si l'une au moins des propositions $P$ ou $Q$ est vraie. Par exemple, si les propositions $P$ et $Q$ sont vraies toutes les deux, alors ($P$ ou $Q$) est vraie aussi. Si $P$ et $Q$ sont fausses toutes les deux, alors la proposition ($P$ ou $Q$) est fausse.

Revenons à notre exemple et choisissons $n = 5$ et $p = 3$. Alors la proposition « $np$ est pair » est fausse et la proposition « $n^2 - p^2$ est multiple de 8 » est vraie, donc $R$ est vraie lorsque $n = 5$ et $p = 3$. Si $n = 5$ et $p = 2$, la proposition « $n^2 - p^2$ est multiple de 8 » est fausse et la proposition « $np$ est pair » est vraie, donc $R$ est vraie. Lorsque $n = 6$ et $p = 2$, chacune des deux propositions « $np$ est pair » et « $n^2 - p^2$ est multiple de 8 » est vraie, donc $R$ est vraie aussi dans ce cas. Nous montrerons au paragraphe 2 qu'à chaque fois que l'on choisit des entiers relatifs $n$ et $p$, la proposition $R$ est vraie.

**L'opération « et ».** Considérons la proposition suivante, où $x$ est un nombre réel :

$R$ : « $x$ est strictement positif et $x^2 + 3x - 4$ est strictement négatif ».

Cette proposition est de la forme ($P$ et $Q$) où $P$ est la proposition « $x$ est strictement positif » et où $Q$ est la proposition « $x^2 + 3x - 4$ est strictement négatif ».

Par définition, une proposition de la forme ($P$ et $Q$) est vraie si les propositions $P$ et $Q$ sont toutes les deux vraies. Si la proposition $P$ est fausse ou si la proposition $Q$ est fausse, alors la proposition ($P$ et $Q$) est fausse.

Puisqu'on a $x^2 + 3x - 4 = (x-1)(x+4)$, la proposition « $x^2 + 3x - 4$ est strictement négatif » est vraie si et seulement si le nombre réel $x$ vérifie les inégalités $-4 < x < 1$ ; la proposition $R$ ci-dessus est donc vraie si et seulement si l'on a $0 < x < 1$.

**L'implication.** Si $P$ et $Q$ sont des propositions, la proposition « si $P$, alors $Q$ » exprime que si $P$ est vraie, alors $Q$ est vraie aussi. Les propositions de ce type sont tellement utilisées qu'on leur a donné un nom : on les appelle des *implications*. La

proposition « si $P$, alors $Q$ » peut aussi s'exprimer par « $P$ implique $Q$ » ou encore par « $P$ donc $Q$ ».

Lorsque les propositions $P$ et $Q$ sont constituées de symboles mathématiques, et seulement dans ce cas, on peut utiliser le signe $\Rightarrow$ qui se lit « implique », ou encore « entraîne » et l'on écrit $P \Rightarrow Q$ pour exprimer que la proposition $P$ implique la proposition $Q$.

Voici des exemples de formulations d'implication :

- si $n$ est un entier positif, alors $n^3 - n$ est multiple de 3
- $n$ est un entier positif implique que $n^3 - n$ est multiple de 3
- $6 < 25/4 \Rightarrow \sqrt{6} < 5/2$
- $x$ appartient à l'intervalle $]-4, 1[$, donc $x^2 + 3x - 4$ est strictement négatif
- $x \in ]-\infty, -4[ \Rightarrow x^2 + 3x - 4 > 0$.

Si $P$ et $Q$ sont des propositions, alors la proposition $(P \Rightarrow Q)$ est vraie seulement dans l'un des cas suivants : ou bien $P$ et $Q$ sont vraies, ou bien $P$ est fausse. Ainsi

> La proposition $(P \Rightarrow Q)$ est vraie si et seulement si la proposition $(\text{non}(P)$ ou $Q)$ est vraie.

En particulier, si la proposition $P$ est fausse, alors la proposition $(P \Rightarrow Q)$ est vraie.

**L'équivalence.** La proposition $((P \Rightarrow Q)$ et $(Q \Rightarrow P))$ se note $P \Leftrightarrow Q$. Le signe $\Leftrightarrow$ se lit « équivaut à » ou « si et seulement si ». Si $P$ et $Q$ sont des propositions vraies, alors la proposition $(P \Leftrightarrow Q)$ est vraie ; si $P$ est vraie et $Q$ est fausse, alors la proposition $(P \Leftrightarrow Q)$ est fausse et de même si $P$ est vraie et $Q$ est fausse. Si $P$ et $Q$ sont des propositions fausses, alors la proposition $(P \Leftrightarrow Q)$ est vraie. Lorsque la proposition $(P \Leftrightarrow Q)$ est vraie, on dit aussi que les propositions $P$ et $Q$ sont *équivalentes*. Par exemple, lorsque $z$ et $z'$ sont des nombres complexes, on a l'équivalence

$$zz' = 0 \Longleftrightarrow (z = 0 \quad \text{ou} \quad z' = 0).$$

Si $P$ est une proposition, alors $P$ et $\text{non}(\text{non}(P))$ sont équivalentes. De plus, si $P$, $Q$ et $R$ sont des propositions, on vérifie que l'on a les équivalences :

$$\text{non}(P \text{ ou } Q) \Longleftrightarrow (\text{non}(P) \text{ et } \text{non}(Q))$$
$$\text{non}(P \text{ et } Q) \Longleftrightarrow (\text{non}(P) \text{ ou } \text{non}(Q))$$
$$(P \text{ ou } (Q \text{ et } R)) \Longleftrightarrow ((P \text{ ou } Q) \text{ et } (P \text{ ou } R))$$
$$(P \text{ et } (Q \text{ ou } R)) \Longleftrightarrow ((P \text{ et } Q) \text{ ou } (P \text{ et } R)).$$



Très souvent, une proposition est vraie ou fausse selon les « valeurs » que prennent certaines « variables ». Par exemple, nous avons vu que lorsque $x$ est un nombre réel, la proposition $x^2 + 3x - 4 < 0$ n'est pas toujours vraie : elle ne l'est que lorsque $x$ est un nombre appartenant à l'intervalle $]-4, 1[$. De même, il peut être utile d'affirmer que l'on peut trouver un nombre réel $x$ tel que $x^5 + x - 1 = 0$.

Pour préciser ces différents cas de figure, on dispose des expressions « pour tout » ou bien « quel que soit » qui ont le même sens, et aussi de l'expression « il existe ».

## L'expression « pour tout »

Pour exprimer que l'on a $x^2 + 3x - 4 < 0$ à chaque fois que $x$ est un nombre de l'intervalle $]-4, 1[$, nous dirons « pour tout nombre $x$ appartenant à $]-4, 1[$, on a $x^2 + 3x - 4 < 0$ » ou bien « quel que soit le nombre $x$ appartenant à $]-4, 1[$, on a $x^2 + 3x - 4 < 0$ ». Puisque cette proposition est vraie, la proposition « pour tout $x$ appartenant à $]-2, 1[$, on a $x^2 + 3x - 4 < 0$ » est vraie également. Mais la proposition « pour tout $x$ appartenant à $]0, 3[$, on a $x^2 + 3x - 4 < 0$ » est fausse : en effet, le nombre 2 appartient à $]0, 3[$ et le nombre $2^2 + 3 \times 2 - 4$ n'est pas strictement négatif.

Lorsqu'on veut exprimer par des symboles mathématiques une proposition qui commence par l'expression « pour tout », on utilise le signe $\forall$, qui se lit « pour tout » et le signe $\in$, qui se lit « appartient à » et qui affirme qu'un élément est dans l'ensemble considéré. On écrit $x \in ]-4, 1[$ pour signifier que le nombre réel $x$ satisfait les inégalités $-4 < x < 1$ et notre proposition se formalise de la manière suivante :

$$\forall x \in ]-4, 1[, \quad x^2 + 3x - 4 < 0.$$

Plus généralement, supposons que $P$ est une proposition qui dépend d'un objet appartenant à un certain ensemble $E$. La proposition $(\forall x \in E, P)$ est vraie si et seulement si $P$ est vraie à chaque fois que $x$ est un élément de l'ensemble $E$. Pour que la proposition $(\forall x \in E, P)$ soit fausse, il suffit de trouver un élément $x$ appartenant à $E$ pour lequel la proposition $P$ est fausse.

## L'expression « il existe »

Supposons que l'on veuille affirmer la possibilité de trouver un nombre réel $x$ vérifiant la propriété $x^2 + 53x - 231 = 0$. Nous dirons « il existe un nombre réel $x$ tel que $x^2 + 53x - 231 = 0$ ». En fait, il est facile de calculer deux nombres réels ayant cette propriété ; mais pour être assuré que la proposition précédente est vraie, il suffit de trouver l'un de ces nombres, ou bien sans faire de calculs, d'expliquer pourquoi il est possible d'en trouver un (le discriminant du trinôme est positif).

On peut employer le signe $\exists$, qui se lit « il existe », pour formuler par des symboles une proposition commençant par l'expression « il existe ». Par exemple, on écrit

$$\exists x \in \mathbf{R}, \quad x^2 + 53x - 231 = 0.$$

D'une façon générale, supposons que $P$ est une proposition qui dépend d'un objet appartenant à un certain ensemble $E$. La proposition $(\exists x \in E,\ P)$ est fausse si et seulement si la proposition $P$ est fausse pour tous les éléments de $E$.

**La négation de la proposition $(\forall x \in E,\ P)$ est la proposition $(\exists x \in E,\ \text{non}(P))$.**

Les opérations précédentes permettent de former des propositions assez complexes et néanmoins utiles. Voici des exemples de propositions vraies.

- Si $a$ et $b$ sont des nombres réels tels que $a \neq 0$ ou $b \neq 0$, alors l'équation $x^2 + 2bx - a^2 = 0$ possède deux solutions réelles distinctes.
- Il existe un entier naturel $p$ tel que l'on a $2^n > n^{13}$ pour tout entier naturel $n$ plus grand que $p$.
- Pour tout entier relatif $a$, il existe des entiers relatifs $q$ et $r$ tels que $a = 5q + r$ et $0 \leqslant r < 5$.

**Les signes $\Rightarrow$, $\Leftrightarrow$, $\forall$, $\exists$ ne s'emploient que dans des formules.**

Dans un livre de mathématiques, les propositions à retenir sont en général introduites par le mot **Proposition**. Certaines propositions particulièrement importantes sont signalées par le mot **Théorème**. Un **Corollaire** est une propriété qui résulte facilement d'un théorème ou d'une proposition précédente. Un **Lemme** est une propriété dont on a besoin pour la suite et qui mérite d'être mise en évidence.

## 2. Le raisonnement

Pour affirmer qu'une proposition $Q$ est vraie, on fait un *raisonnement* ou une *démonstration*. Pour cela, on utilise des propositions que l'on sait déjà être vraies et l'on *en déduit* la proposition $Q$ grâce à un petit nombre de règles de raisonnement.

### Le raisonnement direct

Si la proposition $P$ est vraie et si la proposition $(P \Rightarrow Q)$ est vraie, alors la proposition $Q$ est vraie. En effet, supposons que les propositions $P$ et $(P \Rightarrow Q)$ sont vraies. Puisque la proposition $(P \Rightarrow Q)$ est vraie, c'est que la proposition $P$ est fausse ou bien que les propositions $P$ et $Q$ sont toutes les deux vraies ; puisque $P$ est vraie, $P$ n'est pas fausse et donc la proposition $Q$ est vraie. Voici le schéma de cette déduction :

$$(P \text{ et } (P \Rightarrow Q)) \implies Q.$$



Quelquefois, la proposition $(P \Rightarrow Q)$ aura été démontrée dans le cours sous forme d'un théorème ou d'un corollaire. Dans ce cas, il suffit de citer le résultat en question pour être assuré que $P$ implique $Q$. Mais souvent, il faudra démontrer que la proposition $(P \Rightarrow Q)$ est vraie. Pour cela, on fait *l'hypothèse* que la proposition $P$ est vraie et l'on démontre que la proposition $Q$ est vraie. Une démonstration de $(P \Rightarrow Q)$ est introduite par l'expression « Supposons $P$ » et se termine par « donc $Q$ ».

Pour démontrer une proposition de la forme « pour tout $x \in E$, $Q$ », on se donne un élément quelconque $x$ appartenant à l'ensemble $E$ et l'on démontre que la proposition $Q$ est vraie pour cet élément $x$. La démonstration débute par l'expression « Soit $x$ un élément de $E$ » ou bien par « Soit $x \in E$ » et se termine par « donc $Q$ ».

**Exemple.** Démontrons la proposition (5) du paragraphe 1, qui est de la forme

pour tout entier relatif $n$, $16n^2 - 48n + 33$ est un entier positif.

Soit $n$ un entier relatif. Puisqu'un produit, une somme et une différence d'entiers relatifs sont des entiers relatifs, on en déduit que $16n^2 - 48n + 33$ est un entier relatif. D'autre part, on a l'égalité $16n^2 - 48n + 33 = 4(2n-3)^2 - 3$. Puisque $n$ est un entier relatif, $2n - 3$ est un entier relatif différent de 0, par suite on a $|2n-3| \geqslant 1$, d'où $(2n-3)^2 \geqslant 1$. Il s'ensuit que l'on a $4(2n-3)^2 - 3 \geqslant 4 - 3 = 1$, donc $16n^2 - 48n + 33$ est un entier positif.

On a ainsi démontré que pour tout entier relatif $n$, $16n^2 - 48n + 33$ est un entier positif.

Pour démontrer une proposition de la forme « il existe $x \in E$, $Q$ », le plus direct est d'exhiber un élément de l'ensemble $E$ pour lequel la proposition $Q$ est vraie. Mais quelquefois, il n'est pas possible de calculer explicitement un tel élément. Dans ce cas, il faut penser à appliquer un résultat du cours affirmant qu'un tel élément existe. Par exemple, pour démontrer qu'il existe un nombre réel $x$ tel que $x^5 = 1 - x$, on cite un théorème sur les fonctions continues (voir le chapitre 5 du tome d'analyse).

### Le raisonnement cas par cas

Il s'applique lorsqu'on veut démontrer une implication de la forme $((P \text{ ou } Q) \Rightarrow R)$. On distingue deux cas : ou bien $P$ est vraie et il faut démontrer qu'alors $R$ est vraie, ou bien $Q$ est vraie et il faut démontrer qu'alors $R$ est vraie. La structure du raisonnement est

<u>premier cas</u> : supposons que $P$ est vraie ..., donc $R$

<u>second cas</u> : supposons que $Q$ est vraie ..., donc $R$.

**Exemple 1.** Démontrons que pour tout nombre réel $x$, on a $|x-2| < x^2 - 2x + 3$.

Soit $x$ un nombre réel.

Premier cas : $x \geqslant 2$. Il vient $|x-2| = x - 2$ et

$$x^2 - 2x + 3 - |x-2| = x^2 - 3x + 5 = \left(x - \frac{3}{2}\right)^2 + \frac{11}{4} \geqslant \frac{11}{4},$$

donc $x^2 - 2x + 3 - |x-2| > 0$. Par conséquent, on a $|x-2| < x^2 - 2x + 3$.

Second cas : $x < 2$. Dans ce cas, il vient $|x-2| = 2 - x$ et

$$x^2 - 2x + 3 - |x-2| = x^2 - x + 1 = \left(x - \frac{1}{2}\right)^2 + \frac{3}{4} \geqslant \frac{3}{4},$$

donc $x^2 - 2x + 3 - |x-2| > 0$. Par suite on a $|x-2| < x^2 - 2x + 3$.

Nous avons ainsi démontré que l'inégalité $|x-2| < x^2 - 2x + 3$ est vraie quel que soit le nombre réel $x$.

**Exemple 2.** Démontrons que si $n$ et $p$ sont des entiers relatifs, alors $np$ est pair ou $n^2 - p^2$ est multiple de 8.

Soient $n$ et $p$ des entiers relatifs.

Premier cas : l'un au moins des entiers relatifs $n$ ou $p$ est pair. Dans ce cas, le produit $np$ est pair.

Second cas : $n$ et $p$ sont tous les deux impairs. Alors il existe des entiers relatifs $k$ et $\ell$ tels que $n = 2k + 1$ et $p = 2\ell + 1$. Il vient

$$n^2 - p^2 = 4k^2 + 4k + 1 - 4\ell^2 - 4\ell - 1 = 4\big(k(k+1) - \ell(\ell+1)\big).$$

Puisque $k$ et $k+1$ sont des entiers relatifs consécutifs, le produit $k(k+1)$ est pair. Il en est de même du produit $\ell(\ell+1)$. Il s'ensuit que $k(k+1) - \ell(\ell+1)$ est pair, par suite l'entier relatif $n^2 - p^2$ est multiple de 8.

Puisque l'on se trouve toujours dans l'un des deux cas ci-dessus, on a ainsi démontré que pour tous entiers relatifs $n$ et $p$, $np$ est pair ou $n^2 - p^2$ est multiple de 8.

## Le raisonnement par contraposée

Il s'agit d'une règle de raisonnement permettant de démontrer qu'une implication $(P \Rightarrow Q)$ est vraie. Notons $A$ la proposition $(P \Rightarrow Q)$ et $B$ la proposition $(\mathrm{non}(Q) \Rightarrow \mathrm{non}(P))$.

La proposition $A$ est équivalente à $(\mathrm{non}(P)$ ou $Q)$ et la proposition $B$ est équivalente à $(\mathrm{non}(\mathrm{non}(Q))$ ou $\mathrm{non}(P))$, c'est-à-dire à $(Q$ ou $\mathrm{non}(P))$. Il s'ensuit que les propositions $A$ et $B$ sont équivalentes.

La proposition $B$ s'appelle la *contraposée* de la proposition $A$.



Raisonner par contraposée pour démontrer que $A$ est vraie, c'est démontrer que $B$ est vraie. Pour cela, on fait l'hypothèse que $\mathrm{non}(Q)$ est vraie, autrement dit que $Q$ est fausse et l'on démontre que $\mathrm{non}(P)$ est vraie, c'est-à-dire que $P$ est fausse.

**Exemple.** Soient $x$ et $y$ des nombres réels. Démontrons que si $x$ et $y$ sont différents, alors les nombres $(x+1)(y-1)$ et $(x-1)(y+1)$ sont différents. Il s'agit de démontrer l'implication

$$(x \neq y) \Longrightarrow \big((x+1)(y-1) \neq (x-1)(y+1)\big).$$

Il revient au même de démontrer la contraposée de cette proposition, c'est-à-dire de démontrer l'implication

$$\big((x+1)(y-1) = (x-1)(y+1)\big) \Longrightarrow (x = y).$$

Supposons l'égalité $(x+1)(y-1) = (x-1)(y+1)$ vraie, c'est-à-dire supposons que l'on a $xy - x + y - 1 = xy + x - y - 1$. En simplifiant par $xy - 1$, il vient $-x + y = x - y$, d'où $2(x-y) = 0$. On en déduit $x - y = 0$, ou encore $x = y$.

## Le raisonnement par l'absurde

Pour démontrer l'implication $(P \Rightarrow Q)$ en raisonnant par l'absurde, on fait les hypothèses que $P$ est vraie et que $Q$ est fausse ; on cherche alors une proposition $A$ qui sous ces hypothèses, serait à la fois vraie et fausse, ce qui n'est pas possible : on dit que c'est une *contradiction* ou que c'est *contradictoire*. Les deux hypothèses $P$ vraie et $Q$ fausse ne peuvent donc pas être vérifiées en même temps. Cela signifie que l'une des deux au moins n'est pas vraie, autrement dit $P$ est fausse ou bien $Q$ est vraie. Cette affirmation exprime exactement que l'implication $(P \Rightarrow Q)$ est vraie.

Si au cours de la démonstration de $(P \Rightarrow Q)$ en raisonnant par l'absurde, vous ne vous servez pas que $P$ est effectivement vraie, c'est qu'il fallait raisonner par contraposée.

**Exemple.** Démontrons, en raisonnant par l'absurde, que si $n$ est un entier positif, alors $n^2+1$ n'est pas le carré d'un entier naturel. Supposons que $n$ est un entier positif et que $n^2+1$ est le carré d'un entier naturel $a$. On a alors $n^2+1=a^2$, donc $a^2-n^2=1$, c'est-à-dire $(a-n)(a+n)=1$. Puisque le produit de ces deux nombres est égal à 1, $a+n$ est différent de 0. Or $a+n$ est un entier relatif et puisque nous avons supposé $a$ positif ou nul, on a $a+n \geqslant n > 0$ et donc $a+n$ est un entier positif. Il s'ensuit que $a-n$ est un entier positif. Un produit d'entiers positifs n'est égal à 1 que si chacun d'entre eux est égal à 1. On en déduit $a-n=1$, ou encore $a=n+1$. Il vient $a^2=n^2+2n+1$ et $a^2=n^2+1$, d'où par soustraction $2n=0$. Puisque $n$ est positif, cela est une contradiction.

## Le raisonnement par récurrence

Soit $a$ un entier naturel. Supposons que pour tout entier $n$ supérieur ou égal à $a$, nous ayons défini une propriété qui dépend de $n$ et qu'il est donc commode de noter $\mathscr{P}_n$.

**Principe de récurrence.** *Si la propriété $\mathscr{P}_a$ est vraie et si pour tout entier naturel $n$ supérieur ou égal à $a$, on a l'implication $(\mathscr{P}_n \Rightarrow \mathscr{P}_{n+1})$, alors la propriété $\mathscr{P}_n$ est vraie quel que soit l'entier naturel $n$ supérieur ou égal à $a$.*

Le principe de récurrence fait partie des propriétés caractéristiques de l'ensemble des entiers naturels.

**Exemple 1.** Démontrons que pour tout entier naturel $n$, on a l'inégalité $2^n > n$, en raisonnant par récurrence. Soit $\mathscr{P}_n$ la propriété : $2^n > n$.

On a $2^0 = 1$ et $1 > 0$, donc la propriété $\mathscr{P}_0$ est vraie.

Soit $n$ un entier naturel. Supposons la propriété $\mathscr{P}_n$ vraie et démontrons la propriété $\mathscr{P}_{n+1}$. On a $2^{n+1} = 2^n \times 2 = 2^n + 2^n$. Par hypothèse, on a l'inégalité $2^n > n$. On en déduit l'inégalité $2^{n+1} > n + 2^n$. Puisqu'on a $2^n \geqslant 1$, il vient $2^{n+1} > n + 1$.

Nous avons ainsi démontré que pour tout entier naturel $n$, l'implication $(\mathscr{P}_n \Rightarrow \mathscr{P}_{n+1})$ est vraie. Puisque la propriété $\mathscr{P}_0$ est vraie, le principe de récurrence affirme que l'inégalité $2^n > n$ est vraie quel que soit l'entier naturel $n$.

**Exemple 2.** Pour tout entier naturel $n$ supérieur ou égal à 2, posons

$$S_n = 1 \times 2 + 2 \times 3 + \cdots + (n-1) \times n.$$

Le signe $\cdots$ signifie que $S_n$ est la somme des $n-1$ premiers produits de deux entiers naturels consécutifs, depuis $1 \times 2$ jusqu'a $(n-1) \times n$. Démontrons que l'on a $S_n = \frac{1}{3}n(n-1)(n+1)$ pour tout entier naturel $n \geqslant 2$, en raisonnant par récurrence.

Soit $\mathscr{P}_n$ la propriété : $S_n = \frac{1}{3}n(n-1)(n+1)$. La propriété $\mathscr{P}_2$ est vraie car on a $S_2 = 1 \times 2 = 2$ et $\frac{1}{3} \times 2(2-1)(2+1) = 2$. Soit $n$ un entier naturel supérieur ou égal à 2. Supposons la propriété $\mathscr{P}_n$ vraie et démontrons la propriété $\mathscr{P}_{n+1}$. Par hypothèse, on a l'égalité $S_n = \frac{1}{3}n(n-1)(n+1)$. D'autre part, par définition, nous avons $S_{n+1} = S_n + n(n+1)$, donc il vient

$$S_{n+1} = \frac{n(n-1)(n+1)}{3} + n(n+1) = \frac{n(n-1)(n+1) + 3n(n+1)}{3}$$
$$= \frac{n(n+1)(n-1+3)}{3} = \frac{n(n+1)(n+2)}{3}.$$

Puisqu'on a $n(n+1)(n+2) = (n+1)\big((n+1)-1\big)\big((n+1)+1\big)$, la propriété $\mathscr{P}_{n+1}$ est vraie. Nous avons ainsi démontré que pour tout entier naturel $n$ supérieur ou égal à 2, l'implication $(\mathscr{P}_n \Rightarrow \mathscr{P}_{n+1})$ est vraie. Le principe de récurrence affirme que l'égalité $S_n = \frac{1}{3}n(n-1)(n+1)$ est vraie pour tout entier naturel $n$ supérieur ou égal à 2.

**Exemple 3.** Démontrons, en raisonnant par récurrence, que pour tout entier naturel $n$ supérieur ou égal à 5, on a l'inégalité $2^n > n^2$. Soit $\mathscr{P}_n$ la propriété : $2^n > n^2$. On a $2^5 = 32$ et $5^2 = 25$, par suite la propriété $\mathscr{P}_5$ est vraie. Soit $n$ un entier naturel supérieur ou égal à 5. Supposons la propriété $\mathscr{P}_n$ vraie et démontrons la propriété $\mathscr{P}_{n+1}$. Puisqu'on a $2^{n+1} = 2^n + 2^n$ et $2^n > n^2$ par hypothèse, on en déduit $2^{n+1} > 2n^2$. D'autre part, il vient

$$2n^2 - (n+1)^2 = n^2 - 2n - 1 = (n-1)^2 - 2.$$

Or on a $n \geqslant 5$, donc *a fortiori* $n \geqslant 3$. Il s'ensuit $n - 1 \geqslant 2$, puis $(n-1)^2 \geqslant 4$. On en déduit $2n^2 > (n+1)^2$ et donc $2^{n+1} > (n+1)^2$. Nous avons ainsi démontré que pour tout entier naturel $n$ supérieur ou égal à 5, l'implication $(\mathscr{P}_n \Rightarrow \mathscr{P}_{n+1})$ est vraie. Le principe de récurrence affirme que l'inégalité $2^n > n^2$ est vraie quel que soit l'entier naturel $n$ supérieur ou égal à 5.

**Remarque**

Dans l'exemple 3, nous avons démontré que l'implication $(\mathscr{P}_n \Rightarrow \mathscr{P}_{n+1})$ est vraie pour tout entier naturel $n$ supérieur ou égal à 3. Mais les propriétés $\mathscr{P}_3$ et $\mathscr{P}_4$ sont fausses.

**Exemple 4.** Soit $(u_n)_{n\in\mathbb{N}}$ la suite d'entiers naturels définie par $u_0 = 1$, $u_1 = 3$ et $u_{n+2} = 4u_n + u_{n+1}$ quel que soit $n \in \mathbb{N}$. Démontrons, en raisonnant par récurrence, que pour tout entier naturel $n$, on a $u_n \leqslant 3^n$. Soit $\mathscr{P}_n$ la propriété : $u_n \leqslant 3^n$ et $u_{n+1} \leqslant 3^{n+1}$. Puisqu'on a $u_0 = 1$ et $u_1 = 3$, la propriété $\mathscr{P}_0$ est vraie. Soit $n$ un entier naturel. Supposons que la propriété $\mathscr{P}_n$ est vraie. On a alors

$$\begin{aligned} u_{n+2} = 4u_n + u_{n+1} &\leqslant 4 \times 3^n + 3^{n+1} && \text{par hypothèse} \\ &\leqslant 3^n + 3 \times 3^n + 3^{n+1} \\ &\leqslant 3^{n+1} + 3^{n+1} + 3^{n+1} && \text{car } 3^n \leqslant 3^{n+1} \\ &\leqslant 3 \times 3^{n+1}, \end{aligned}$$

c'est-à-dire $u_{n+2} \leqslant 3^{n+2}$. Nous avons ainsi démontré que pour tout entier naturel $n$, l'implication $(\mathscr{P}_n \Rightarrow \mathscr{P}_{n+1})$ est vraie. D'après le principe de récurrence, la propriété $\mathscr{P}_n$ est vraie quel que soit $n \in \mathbb{N}$. En particulier, on a $u_n \leqslant 3^n$ quel que soit $n \in \mathbb{N}$.

## Exercices

1. Pour quelles valeurs du nombre réel $x$ la proposition
$$(2x^2 + 5x - 12 < 0 \quad \text{ou} \quad x^2 + 3x + 2 > 0)$$
est-elle vraie ?

2. Trouver tous les nombres réels $x$ tels que $\sqrt{x+3} > x + 1$.

3. Trouver tous les couples $(x, y)$ de nombres réels tels que
$$\begin{cases} x(x^2 + y^2 - 1) = 0 \\ y(x + y + 1) = 0. \end{cases}$$

4. Pour tout entier positif $n$, notons $s_n$ la somme des $n$ premiers carrés d'entiers positifs, de sorte que l'on a $s_1 = 1^2$, $s_2 = 1^2 + 2^2$, $s_3 = 1^2 + 2^2 + 3^2$ et plus généralement
$$s_n = 1^2 + 2^2 + \cdots + n^2.$$
Démontrer que pour tout entier positif $n$, on a $s_n = \dfrac{n(n+1)(2n+1)}{6}$.

5. On définit la suite $(f_n)_{n \geqslant 0}$ de fonctions polynômes de la manière suivante :
$$f_0(x) = 2, \quad f_1(x) = x \quad \text{et} \quad f_{n+2}(x) = x f_{n+1}(x) - f_n(x)$$
pour tout nombre réel $x$ et pour tout entier naturel $n$.

**a)** Calculer $f_2(x)$ et $f_3(x)$.

**b)** Démontrer que pour tout entier naturel $n$ et pour tout nombre réel $x$ non nul, on a
$$f_n\left(x + \frac{1}{x}\right) = x^n + \frac{1}{x^n}.$$

6. Les propositions suivantes sont-elles vraies ou fausses ? Justifiez votre réponse en faisant une démonstration.

**a)** $\forall x \in \mathbf{R}$ , $(x = |x|$ ou $x = -|x|)$.

**b)** $(\forall x \in \mathbf{R}$ , $x = |x|)$ ou $(\forall x \in \mathbf{R}$ , $x = -|x|)$.

**c)** $\forall x \in \mathbf{Z}$ , $\exists y \in \mathbf{Z}$ , $y - x + x^2 < 0$.

**d)** $\exists y \in \mathbf{Z}$ , $\forall x \in \mathbf{Z}$ , $y - x + x^2 < 0$.

**e)** $\exists y \in \mathbf{Z}$ , $\forall x \in \mathbf{Z}$ , $y - x + x^2 > 0$.

7. Pour tout entier naturel $a$, on définit les propositions suivantes :
$$P(a) \ : \ (\forall x \in \mathbf{R}, \quad x^2 + 2ax + 8 \geqslant 0) \Rightarrow (\forall x \in \mathbf{R}, \quad x^2 + 2x + 3 \geqslant a)$$
$$Q(a) \ : \ \forall x \in \mathbf{R}, \quad (x^2 + 2ax + 8 \geqslant 0 \Rightarrow x^2 + 2x + 3 \geqslant a).$$

**a)** Montrer que la proposition $P(a)$ est vraie quel que soit l'entier naturel $a$.

**b)** La proposition $Q(a)$ est-elle vraie quel que soit l'entier naturel $a$ ?



8. Si $x$ est un nombre réel, la *partie entière* de $x$, notée $E(x)$, est le plus grand entier inférieur ou égal à $x$ ; cet entier est caractérisé par la double inégalité $E(x) \leqslant x < E(x) + 1$. Soit $n$ un entier au moins égal à 2.

**a)** Montrer que l'on a $E(x+1) = E(x) + 1$ pour tout nombre réel $x$.

**b)** Pour tout nombre réel $x \geqslant 0$, posons
$$f(x) = E(x) + E\left(x + \frac{1}{n}\right) + E\left(x + \frac{2}{n}\right) + \cdots + E\left(x + \frac{n-1}{n}\right) \quad \text{et} \quad g(x) = E(nx).$$
Montrer que l'on a $f\left(x + \frac{1}{n}\right) - g\left(x + \frac{1}{n}\right) = f(x) - g(x)$.

**c)** On suppose $0 \leqslant x < 1/n$. Calculer $f(x)$ et $g(x)$.

**d)** Soit $a$ un nombre réel positif ou nul. Montrer que l'on a
$$E(na) = E(a) + E\left(a + \frac{1}{n}\right) + E\left(a + \frac{2}{n}\right) + \cdots + E\left(a + \frac{n-1}{n}\right).$$

## Quelques réponses ou indications

3. Un couple $(x, y)$ de nombres réels est solution si et seulement si les propositions $P : x(x^2 + y^2 - 1) = 0$ et $Q : y(x + y + 1) = 0$ sont toutes les deux vraies. La proposition $P$ est équivalente à $(A$ ou $B)$, où $A$ est la proposition $(x = 0)$ et où $B$ est la proposition $(x^2 + y^2 - 1 = 0)$. Les solutions sont donc les couples $(x, y)$ pour lesquels l'une au moins des propositions $(A$ et $Q)$, $(B$ et $Q)$ est vraie. Décomposer de même la proposition $Q$ en $(C$ ou $D)$. Un couple $(x, y)$ est solution si et seulement si l'une au moins des propositions $(A$ et $C)$, $(B$ et $C)$, $(A$ et $D)$, $(B$ et $D)$ est vraie.

4. Raisonner par récurrence.

5. Pour tout entier naturel $n$, soit $\mathscr{P}_n$ la propriété :
$$f_n\left(x + \frac{1}{x}\right) = x^n + \frac{1}{x^n} \quad \text{et} \quad f_{n+1}\left(x + \frac{1}{x}\right) = x^{n+1} + \frac{1}{x^{n+1}}.$$
En raisonnant par récurrence, démontrer que pour tout entier naturel $n$, la propriété $\mathscr{P}_n$ est vraie.

6. **a)** Pour tout $x \in \mathbf{Z}$, on a $x - x^2 \leqslant 0$.

7. **a)** Déterminer les entiers naturels $a$ tels que l'on ait $x^2 + 2ax + 8 \geqslant 0$ quel que soit $x \in \mathbf{R}$, puis les entiers naturels $a$ tels que l'on ait $x^2 + 2x + 3 - a \geqslant 0$ quel que soit $x \in \mathbf{R}$.

**b)** Montrer que la proposition $Q(3)$ est fausse.

8. c) On a $f(x) = 0$ et $g(x) = 0$.

d) Pour tout entier $k \geqslant 1$, définissons la propriété $\mathscr{P}_k$ suivante :

quel que soit le nombre réel $x$ tel que $0 \leqslant x < \frac{k}{n}$, on a $f(x) = g(x)$.

La propriété $\mathscr{P}_1$ est vraie, d'après (c). Supposons que $k$ est un entier pour lequel $\mathscr{P}_k$ est vraie. Soit $x$ un nombre réel tel que $0 \leqslant x < \frac{k+1}{n}$. Alors par hypothèse, on a $f(x - 1/n) = g(x - 1/n)$. En utilisant (b), on en déduit $f(x) = g(x)$. D'après le principe de récurrence, la propriété $\mathscr{P}_k$ est donc vraie quel que soit l'entier $k \geqslant 1$. Il s'ensuit que l'on a $f(x) = g(x)$ quel que soit le nombre réel $x \geqslant 0$.



# Chapitre 2

# Ensembles et applications

Dans ce chapitre, nous introduisons le langage des ensembles et des applications. Ces notions de base, essentielles, sont utilisées dans toutes les mathématiques. C'est pourquoi les paragraphes 2 et 3 de ce chapitre devront être une référence permanente, aussi bien en analyse qu'en algèbre. Le dernier paragraphe est une introduction au dénombrement.

## 1. Ensembles fondamentaux

Ces ensembles sont $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$. Les éléments de $\mathbb{N}$ sont les *entiers naturels*, c'est-à-dire $0, 1, 2, 3, \ldots$. Les éléments de $\mathbb{N}$ différents de $0$ sont appelés les *entiers positifs*. Les éléments de $\mathbb{Z}$ sont les *entiers relatifs*, c'est-à-dire $0, 1, -1, 2, -2, \ldots$. Les propriétés arithmétiques des entiers relatifs, c'est-à-dire les propriétés concernant la divisibilité, seront étudiées au chapitre 9. Les éléments de $\mathbb{Q}$ sont les *nombres rationnels*. Rappelons qu'un nombre rationnel s'écrit $a/b$, où $a$ est un entier relatif et où $b$ est un entier positif. De plus, on a $a/b = c/d$ si et seulement si $ad = bc$. Les propriétés de l'ensemble $\mathbb{R}$ des *nombres réels* font l'objet du tome d'analyse. Enfin, l'ensemble $\mathbb{C}$ des *nombres complexes* sera présenté au chapitre suivant.

Au niveau élémentaire où nous nous plaçons, aucune construction de ces ensembles ne sera donnée.

## 2. Opérations sur les ensembles

Il y a deux façons de décrire un ensemble : ou bien en se donnant la liste de ses éléments, ou bien en se donnant une propriété qui caractérise les éléments de cet

ensemble. Par exemple, l'ensemble $\{0, 2, 4, 6, 8\}$ est l'ensemble des chiffres des unités des entiers pairs.

Si $a$ est un élément de l'ensemble $E$, on dit aussi que *$a$ appartient à $E$* ou que *$E$ contient $a$* ; cette propriété se note $a \in E$. Si $a$ n'appartient pas à $E$, ou si $E$ ne contient pas $a$, on écrit $a \notin E$.

Lorsqu'on veut se donner un élément (quelconque) de l'ensemble $E$, par exemple pour commencer une démonstration, on écrit « soit $x$ un élément de $E$ » ou « soit $x \in E$ ».

Si l'on veut se donner des éléments $x$ et $y$ de l'ensemble $E$, alors par abus de notation, on peut écrire « soient $x, y \in E$ ». Attention, cette écriture ne veut pas dire que $x$ est différent de $y$. On peut également écrire « soient $x_1$ et $x_2$ des éléments de $E$ » et plus généralement, si $n$ est un entier supérieur ou égal à 2, « soient $x_1, x_2, \ldots, x_n$ des éléments de $E$ ».

Pour décrire un ensemble dont les éléments vérifient une certaine propriété, plutôt que de faire une phrase, on a souvent recours à une écriture mathématique. Par exemple, l'intervalle $[0, 1]$ est l'ensemble des nombres réels $x$ tels que $0 \leqslant x \leqslant 1$, ce qui s'écrit $[0, 1] = \{ x \in \mathbb{R} \mid 0 \leqslant x \leqslant 1 \}$ ; le trait vertical veut dire et se lit « tel que ».

**Notation.** L'ensemble qui n'a aucun élément s'appelle l'*ensemble vide* et se note $\varnothing$.

**Définition**

Soient $E$ et $F$ des ensembles. Lorsque tout élément de $E$ appartient à $F$, on dit que $E$ est *inclus* dans $F$, ou que $E$ est une *partie* de $F$. Cette propriété se note $E \subset F$.

Pour démontrer l'inclusion $E \subset F$, on doit donc démontrer que tout élément de $E$ appartient à $F$. Pour faire cette démonstration, on se donne un élément (quelconque) de $E$ et l'on prouve qu'il appartient à $F$.

**Exemple.** Considérons les ensembles $E = [2, 3]$, $F = \{ x \in \mathbb{R} \mid x^2 - 3x - 10 < 0 \}$ et démontrons l'inclusion $E \subset F$. Le discriminant du trinôme $x^2 - 3x - 10$ est $49 = 7^2$, les racines sont $-2$ et 5, d'où la factorisation $x^2 - 3x - 10 = (x + 2)(x - 5)$. Supposons que $x$ est un élément de $E$. On a $x \geqslant 2$, donc $x + 2 \geqslant 4$ et *a fortiori* $x + 2 > 0$. De plus, on a $x \leqslant 3$ et par suite $x - 5 \leqslant -2$. On en déduit $x - 5 < 0$, donc $(x + 2)(x - 5) < 0$, c'est-à-dire $x^2 - 3x - 10 < 0$. On a donc démontré que pour tout $x \in E$, on a $x \in F$, d'où l'inclusion $E \subset F$. Mais attention, l'ensemble $E$ n'est pas égal à $F$ : le nombre réel 0 appartient à $F$ et n'appartient pas à $E$.



**Remarque importante**

Des ensembles $E$ et $F$ sont égaux si et seulement si on a les deux inclusions $E \subset F$ et $F \subset E$. Dans la pratique, lorsqu'on doit démontrer l'égalité de deux ensembles, il faut prouver les deux inclusions.

**Exemple.** L'ensemble $F = \{ x \in \mathbb{R} \mid x^2 - 3x - 10 < 0 \}$ est égal à l'intervalle $]-2, 5[$.

**Notation.** L'ensemble des parties de l'ensemble $E$ se note $\mathscr{P}(E)$.

**Exemple.** Soit l'ensemble $E = \{1, 2\}$. Les parties de $E$ sont $\varnothing$, $\{1\}$, $\{2\}$ et $E$. On a donc $\mathscr{P}(E) = \{ \varnothing, \{1\}, \{2\}, \{1, 2\} \}$.

Nous allons maintenant définir des opérations sur les parties d'un ensemble.

**Définition**

Soit $E$ un ensemble. Pour toute partie $A$ de $E$, l'ensemble des éléments de $E$ qui n'appartiennent pas à $A$ s'appelle le *complémentaire* de $A$ et se note $\complement_E A$, ou plus simplement $\complement A$, ou encore $E \setminus A$.

**Définitions**

Soit $E$ un ensemble. Pour toutes parties $A$ et $B$ de $E$,

- l'ensemble des éléments de $E$ qui appartiennent à $A$ et à $B$ s'appelle l'*intersection* de $A$ et $B$ et se note $A \cap B$ (ce qui se lit « $A$ inter $B$ ») ;
- l'ensemble des éléments de $E$ qui appartiennent à $A$ ou à $B$ s'appelle la *réunion* de $A$ et $B$ et se note $A \cup B$ (ce qui se lit « $A$ union $B$ »).

Pour toutes parties $A$, $B$ et $C$ de l'ensemble $E$, nous avons les règles de calcul suivantes :

$A \cap B = B \cap A$
$A \cap (B \cap C) = (A \cap B) \cap C$ et cet ensemble est noté $A \cap B \cap C$
$A \cap \varnothing = \varnothing, \quad A \cap A = A, \quad (A \subset B \Leftrightarrow A \cap B = A)$
$A \cup B = B \cup A$
$A \cup (B \cup C) = (A \cup B) \cup C$ et cet ensemble est noté $A \cup B \cup C$
$A \cup \varnothing = A, \quad A \cup A = A, \quad (A \subset B \Leftrightarrow A \cup B = B)$
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
$\complement(\complement A) = A, \quad (A \subset B \Leftrightarrow \complement B \subset \complement A)$
$\complement(A \cap B) = \complement A \cup \complement B, \quad \complement(A \cup B) = \complement A \cap \complement B.$

**Produit cartésien**

Si $E$ et $F$ sont des ensembles, le *produit cartésien* de $E$ par $F$, noté $E \times F$, est l'ensemble des *couples* $(x, y)$, où $x$ décrit $E$ et où $y$ décrit $F$. Les couples $(x, y)$ et $(x', y')$ sont égaux si et seulement si on a $x = x'$ et $y = y'$.

Si $E$ est un ensemble, le produit cartésien $E \times E$ se note $E^2$. Par exemple, le produit cartésien $\mathbb{R}^2$ est formé des couples de nombres réels ; ceux-ci permettent de déterminer un point du plan par ses coordonnées, lorsqu'on s'est donné un repère cartésien.

Plus généralement, pour tout entier $n$ supérieur ou égal à 2, le produit cartésien de $E$ par lui-même $n$ fois se note $E^n$. Les éléments de $E^n$ sont les *n-uples* $(x_1, x_2, \ldots, x_n)$, où les éléments $x_1, x_2, \ldots, x_n$ appartiennent à $E$ ; les $n$-uples $(x_1, x_2, \ldots, x_n)$ et $(y_1, y_2, \ldots, y_n)$ sont égaux si et seulement si on a $x_i = y_i$ pour tout $i \in \{1, 2, \ldots, n\}$.

# 3. Application d'un ensemble dans un autre

Soient $E$ et $F$ des ensembles. Se donner une application $f$ de $E$ dans $F$ c'est définir, pour tout élément $x$ de $E$, un unique élément de $F$, que l'on note $f(x)$ et qui s'appelle l'*image* par $f$ de $x$. On dit qu'à tout élément $x$ de $E$, on associe l'élément $f(x)$ de $F$, ce que l'on note $x \mapsto f(x)$. L'ensemble $E$ s'appelle l'*ensemble de départ* et l'ensemble $F$ s'appelle l'*ensemble d'arrivée* de $f$.

Lorsqu'on se donne une application $f$ de $E$ dans $F$, on écrit « soit $f : E \to F$ une application ». Pour se donner, par exemple, l'application $f$ de $\mathbb{R}$ dans $\mathbb{R}$ qui à tout nombre réel $x$ associe $x^2$, on écrit également : soit l'application

$$f : \mathbb{R} \longrightarrow \mathbb{R}$$
$$x \longmapsto x^2 .$$

**Notation.** Pour tout ensemble $E$, l'application de $E$ dans $E$ qui à tout élément $x$ associe $x$, se note $\mathrm{id}_E$ et s'appelle l'*application identique* de $E$.

**Égalité de deux applications.** Si $E$, $F$, $E'$, $F'$ sont des ensembles et si $f : E \to F$, $f' : E' \to F'$ sont des applications, les applications $f$ et $f'$ sont égales si et seulement si on a $E' = E$, $F' = F$ et $f'(x) = f(x)$ pour tout $x \in E$.

**Définition**
Soient $E$, $F$ des ensembles et $f : E \to F$ une application. Le *graphe* de $f$ est la partie $G$ de $E \times F$ constituée des éléments de la forme $(x, f(x))$, où $x \in E$.



**Définition**
Soient $E$, $F$, $G$ des ensembles et $f : E \to F$, $g : F \to G$ des applications. La *composée* de $f$ et $g$, notée $g \circ f$ (ce qui se lit « $g$ rond $f$ »), est l'application de $E$ dans $G$ définie par $g \circ f(x) = g(f(x))$ pour tout $x \in E$.

**Exemples**

- Pour tous ensembles $E$, $F$ et pour toute application $f : E \to F$, on a $f \circ \mathrm{id}_E = f$ et $\mathrm{id}_F \circ f = f$.
- Soient les applications $f : ]0, +\infty[ \to ]0, +\infty[$ et $g : ]0, +\infty[ \to \mathbb{R}$ définies par $f(x) = 1/x$ et $g(x) = \frac{x-1}{x+1}$ pour tout nombre $x > 0$. Alors on a

$$g \circ f(x) = g(1/x) = \frac{(1/x) - 1}{(1/x) + 1} = \frac{1 - x}{1 + x} = -g(x)$$

pour tout nombre $x > 0$.

**Proposition.** *Soient $E, F, G, H$ des ensembles et $f : E \to F$, $g : F \to G$, $h : G \to H$ des applications. Alors on a $h \circ (g \circ f) = (h \circ g) \circ f$ et cette application se note $h \circ g \circ f$.*

**Démonstration.** Par définition de la composition d'applications, il vient $h \circ (g \circ f)(x) = h(g \circ f(x)) = h(g(f(x)))$ et $(h \circ g) \circ f(x) = h \circ g(f(x)) = h(g(f(x)))$ pour tout $x \in E$, d'où l'égalité cherchée. ∎

**Définitions**
Soient $E$, $F$ des ensembles et $f : E \to F$ une application. On dit que

- l'application $f$ est *injective*, ou que $f$ est une *injection*, si pour tous $x, x' \in E$, on a l'implication $(f(x) = f(x') \Rightarrow x = x')$
- l'application $f$ est *surjective*, ou que $f$ est une *surjection*, si pour tout $y \in F$, il existe $x \in E$ tel que $f(x) = y$
- l'application $f$ est *bijective*, ou que $f$ est une *bijection* de $E$ sur $F$, si pour tout $y \in F$, il existe un unique $x \in E$ tel que $f(x) = y$.

**Remarques**

- Pour démontrer qu'une application $f : E \to F$ n'est pas injective, il suffit d'exhiber des éléments $x$ et $x'$ appartenant à $E$ tels que $x \neq x'$ et $f(x) = f(x')$.
- Pour démontrer qu'une application $f : E \to F$ est injective, il est parfois plus facile de raisonner par contraposée, c'est-à-dire de prouver que pour tous $x, x' \in E$, on a l'implication $(x \neq x' \Rightarrow f(x) \neq f(x'))$.

**Proposition.** *Soient $E$, $F$ des ensembles et $f : E \to F$ une application. L'application $f$ est bijective si et seulement si l'application $f$ est injective et surjective.*

**Démonstration.** Supposons l'application $f$ bijective. Alors en particulier pour tout $y \in F$, il existe $x \in E$ tel que $f(x) = y$ ; l'application $f$ est donc surjective. Soient $x, x' \in E$ tels que $f(x) = f(x')$. Posons $y = f(x)$ : $x$ est l'unique élément de $E$ dont l'image par $f$ est égale à $y$. Puisque $f(x') = y$, on en déduit $x' = x$. On a donc démontré que l'application $f$ est injective.

Réciproquement, supposons l'application $f$ injective et surjective. Soit $y \in F$. Puisque l'application $f$ est surjective, il existe $x \in E$ tel que $f(x) = y$. Si $x'$ est *a priori* un autre élément de $E$ tel que $f(x') = y$, on a $f(x) = f(x')$ et donc $x = x'$, car l'application $f$ est injective. Nous avons ainsi démontré qu'il existe un unique élément de $E$ dont l'image par $f$ est égale à $y$. L'application $f$ est donc bijective. ∎

**Proposition.** *Soient $E$, $F$ des ensembles et $f : E \to F$ une application.*

- *L'application $f$ est bijective si et seulement s'il existe une application $g : F \to E$ telle que $f \circ g = \mathrm{id}_F$ et $g \circ f = \mathrm{id}_E$.*
- *Supposons que $f$ est une bijection. Alors l'application $g$ est unique et bijective. L'application $g$ s'appelle la bijection réciproque de $f$ et se note $f^{-1}$. De plus on a $(f^{-1})^{-1} = f$.*

**Démonstration.** Supposons l'application $f$ bijective et démontrons l'existence et l'unicité de $g$. Pour tout $y \in F$, il existe un unique élément appartenant à $E$ dont l'image par $f$ est égale à $y$ ; notons $g(y)$ cet élément de $E$. On définit ainsi une application $g : F \to E$ telle que $f(g(y)) = y$ pour tout $y \in F$, c'est-à-dire telle que $f \circ g = \mathrm{id}_F$. Composons (à droite) cette égalité avec l'application $f$. Il vient $f \circ g \circ f = \mathrm{id}_F \circ f = f$. Pour tout $x \in E$, on a donc $f(g \circ f(x)) = f(x)$. Puisque l'application $f$ est injective, on en déduit $g \circ f(x) = x$ pour tout $x \in E$. Par conséquent on a l'égalité $g \circ f = \mathrm{id}_E$. Supposons que $h : F \to E$ est *a priori* une autre application telle que $f \circ h = \mathrm{id}_F$ et $h \circ f = \mathrm{id}_E$. En particulier on a $f \circ h = f \circ g$, c'est-à-dire $f(h(x)) = f(g(x))$ pour tout $x \in E$. L'application $f$ étant injective, il s'ensuit $h(x) = g(x)$ pour tout $x \in E$, c'est-à-dire $h = g$.

Supposons que l'application $g$ existe et démontrons que $f$ est une bijection. Si $x$ et $x'$ sont des éléments de $E$ tels que $f(x) = f(x')$, il vient $g(f(x)) = g(f(x'))$, c'est-à-dire $g \circ f(x) = g \circ f(x')$. Puisqu'on a $g \circ f = \mathrm{id}_E$ par hypothèse, cette égalité s'écrit $x = x'$. Cela montre que l'application $f$ est injective. D'autre part, pour tout élément $y \in F$, on a $f(g(y)) = f \circ g(y) = \mathrm{id}_F(y) = y$. L'élément $g(y) \in E$ a donc pour image $y$ par l'application $f$. Par conséquent l'application $f$ est surjective. L'application $f$ est donc injective et surjective, par suite $f$ est une bijection.

Supposons que $f$ est une bijection. On a $g \circ f = \mathrm{id}_E$ et $f \circ g = \mathrm{id}_F$. En appliquant à $g$ ce que nous venons juste de démontrer, on en déduit que $g$ est une bijection. Par définition de la bijection réciproque, il vient alors $g^{-1} = f$. ∎



**Exemple.** Pour tout nombre réel $x$ différent de $-2$, on a $\frac{x+1}{x+2} \neq 1$. En effet, l'égalité $1 - \frac{x+1}{x+2} = \frac{1}{x+2}$ implique $1 - \frac{x+1}{x+2} \neq 0$. Considérons l'application

$$\begin{array}{rcl} f : \mathbf{R} \setminus \{-2\} & \longrightarrow & \mathbf{R} \setminus \{1\} \\ x & \longmapsto & \dfrac{x+1}{x+2} \end{array}$$

et démontrons que $f$ est une bijection. Soient $x$ et $x'$ des nombres réels différents de $-2$ tels que $f(x) = f(x')$. Il vient $(x+1)(x'+2) = (x+2)(x'+1)$. Développons cette égalité : $xx' + 2x + x' + 2 = xx' + x + 2x' + 2$. En simplifiant, on en déduit $x = x'$. L'application $f$ est donc injective. Montrons maintenant que l'application $f$ est surjective. Soit $y$ un nombre réel différent de 1. Cherchons un nombre réel $x$ différent de $-2$ tel que $f(x) = y$. Un tel nombre $x$ doit vérifier $x + 1 = y(x+2)$ et donc $x(1-y) = 2y - 1$. Puisque $y$ est différent de 1, il vient nécessairement $x = \frac{2y-1}{1-y}$. Vérifions maintenant que l'on a $f(x) = y$. Pour cela, il faut avant tout que $f(x)$ soit défini, c'est-à-dire que l'on ait $x \neq -2$. C'est bien le cas, car $\frac{2y-1}{1-y} + 2 = \frac{1}{1-y}$, donc $\frac{2y-1}{1-y} + 2 \neq 0$. Maintenant calculons $f\left(\frac{2y-1}{1-y}\right)$. Il vient effectivement

$$f\left(\frac{2y-1}{1-y}\right) = \frac{(2y-1)/(1-y)+1}{(2y-1)/(1-y)+2} = \frac{(2y-1)+(1-y)}{(2y-1)+2(1-y)} = y.$$

Ainsi l'application $f$ est injective et surjective, donc bijective. De plus, nous avons calculé la bijection réciproque de $f$. C'est l'application

$$\begin{array}{rcl} f^{-1} : \mathbf{R} \setminus \{1\} & \longrightarrow & \mathbf{R} \setminus \{-2\} \\ x & \longmapsto & \dfrac{2x-1}{1-x} \end{array}.$$

**Proposition.** *Soient $E$, $F$, $G$ des ensembles et $f : E \to F$, $g : F \to G$ des bijections. L'application $g \circ f$ est bijective et l'on a $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

**Démonstration.** D'après la proposition précédente, il existe des applications $u : F \to E$ et $v : G \to F$ telles que $f \circ u = \mathrm{id}_F$, $u \circ f = \mathrm{id}_E$, $g \circ v = \mathrm{id}_G$ et $v \circ g = \mathrm{id}_F$. On a $(g \circ f) \circ (u \circ v) = g \circ (f \circ u) \circ v = g \circ \mathrm{id}_F \circ v = g \circ v = \mathrm{id}_G$ et $(u \circ v) \circ (g \circ f) = u \circ (v \circ g) \circ f = u \circ \mathrm{id}_F \circ f = u \circ f = \mathrm{id}_E$. On en déduit, également d'après la proposition précédente, que l'application $g \circ f$ est bijective et que l'on a $(g \circ f)^{-1} = u \circ v = f^{-1} \circ g^{-1}$. ∎

**Définition**

Soient $E$, $F$ des ensembles et $f : E \to F$ une application. Pour toute partie $A$ de $E$, l'*image* de $A$ par $f$ est la partie de $F$, notée $f(A)$, constituée des éléments de $F$ de la forme $f(x)$, où $x \in A$.

En particulier, l'application $f$ est surjective si et seulement si l'image de $E$ par $f$ est égale à $F$ tout entier. Autrement dit l'application $f$ est surjective si et seulement si on a l'égalité $f(E) = F$.

**Exemple.** Soit l'application $f : \mathbb{R} \to \mathbb{R}$ définie par $f(x) = x^2 + 2x$ pour tout $x \in \mathbb{R}$ et soient les ensembles $A = \mathbb{R} \setminus \{-1\}$, $B = ]-1, +\infty[$. Alors on a $f(A) = B$. Pour démontrer cette égalité, nous devons prouver que l'on a $f(A) \subset B$ et $B \subset f(A)$.

Pour tout nombre réel $x$, nous avons $f(x) = (x+1)^2 - 1$. Or pour tout nombre $x \in A$, on a $x + 1 \neq 0$ donc $(x+1)^2 > 0$. On en déduit que pour tout $x \in A$, on a $f(x) > -1$, c'est-à-dire $x \in B$. On a donc l'inclusion $f(A) \subset B$.

Montrons maintenant que $B$ est inclus dans $f(A)$. Soit $y \in B$. On a $y > -1$ et donc $y + 1 > 0$. Posons $x = \sqrt{y+1} - 1$. Nous avons $x \neq -1$, c'est-à-dire $x \in A$. D'autre part on a $f(x) = (x+1)^2 - 1 = \left(\sqrt{y+1}\,\right)^2 - 1 = y$. Par conséquent, $y$ est bien un élément de l'ensemble $f(A)$. Il s'ensuit $B \subset f(A)$.

## 4. Ensembles finis

Dans ce paragraphe, de nombreuses démonstrations se font en raisonnant par récurrence.

**Définition**
Un ensemble $E$ est *fini* s'il est vide ou bien s'il existe un entier positif $n$ et une bijection de $E$ sur l'ensemble des $n$ premiers entiers positifs, noté $\{1, \ldots, n\}$.

Un ensemble qui est en bijection avec un ensemble fini est donc fini.

**Théorème.** *Pour tous entiers positifs $n$ et $k$, s'il existe une injection de $\{1, \ldots, n\}$ dans $\{1, \ldots, k\}$, alors on a $n \leqslant k$.*

**Démonstration.** Pour tout entier positif $n$, notons $\mathscr{P}_n$ la propriété : si $k$ est un entier positif et s'il existe une injection de $\{1, \ldots, n\}$ dans $\{1, \ldots, k\}$, alors on a $n \leqslant k$. Démontrons par récurrence que la propriété $\mathscr{P}_n$ est vraie quel que soit l'entier positif $n$. La propriété $\mathscr{P}_1$ est clairement vraie.

Soit $n$ un entier positif. Supposons la propriété $\mathscr{P}_n$ vraie et démontrons la propriété $\mathscr{P}_{n+1}$. Soient $k$ un entier positif et $f : \{1, \ldots, n+1\} \to \{1, \ldots, k\}$ une application injective. Si $k$ était égal à 1, alors on aurait $f(1) = f(n+1) = 1$, ce qui est impossible car $f$ est une injection et $1 \neq n+1$. On en déduit $k \geqslant 2$. Plus généralement, pour tout $x \in \{1, \ldots, n\}$, on a $f(x) \neq f(n+1)$, puisque l'application $f$ est injective. Remarquons que si $f(x) < f(n+1)$, alors on a $f(x) \in \{1, \ldots, k-1\}$, car $f(x) \leqslant f(n+1) - 1 \leqslant k - 1$. Considérons alors l'application $g : \{1, \ldots, n\} \to \{1, \ldots, k-1\}$ définie par $g(x) = f(x)$ si $f(x) < f(n+1)$ et $g(x) = f(x) - 1$ si $f(x) > f(n+1)$ et démontrons que l'application $g$ est injective. Soient $x, y \in \{1, \ldots, n\}$ tels que $g(x) = g(y)$. Si l'on a $f(x) < f(n+1)$ et $f(y) < f(n+1)$, il vient $g(x) = f(x)$ et $g(y) = f(y)$, d'où $f(x) = f(y)$. Dans ce cas on en déduit $x = y$, puisque $f$ est une injection. Si l'on a $f(x) > f(n+1)$ et $f(y) > f(n+1)$, il vient $g(x) = f(x) - 1$ et $g(y) = f(y) - 1$, donc $f(x) = f(y)$, puis $x = y$ comme précédemment. Démontrons que l'on ne peut pas avoir les inégalités $f(x) < f(n+1) < f(y)$, par exemple (le cas $f(y) < f(n+1) < f(x)$ se traite de la même manière). Si c'était le cas, alors on aurait $g(x) = f(x)$ et $g(y) = f(y) - 1$, d'où $f(y) = f(x) + 1$. L'encadrement $f(x) < f(n+1) < f(y)$ s'écrirait alors $f(x) < f(n+1) < f(x) + 1$. Ainsi l'entier $f(n+1)$ serait strictement compris entre les deux entiers consécutifs $f(x)$ et $f(x) + 1$, ce qui est impossible. Nous avons finalement démontré que $x = y$, par suite l'application $g$ est injective. Par hypothèse de récurrence on a $n \leqslant k - 1$, donc $n + 1 \leqslant k$.

Nous avons ainsi démontré que pour tout entier positif $n$, l'implication $(\mathscr{P}_n \Rightarrow \mathscr{P}_{n+1})$ est vraie. Le principe de récurrence affirme que la propriété $\mathscr{P}_n$ est vraie quel que soit l'entier positif $n$. ∎

**Corollaire.** *Soit $E$ un ensemble fini non vide. Il y a un unique entier positif $n$ pour lequel il existe une bijection de $E$ sur $\{1, \ldots, n\}$.*

**Démonstration.** Par définition, il existe un entier positif $n$ et une bijection $f : E \to \{1, \ldots, n\}$. Supposons que $k$ est un entier positif et qu'il existe une bijection $g : E \to \{1, \ldots, k\}$. La composée de deux bijections étant une bijection, l'application $g \circ f^{-1}$ est une bijection de $\{1, \ldots, n\}$ sur $\{1, \ldots, k\}$ et l'application $f \circ g^{-1}$ est une bijection de $\{1, \ldots, k\}$ sur $\{1, \ldots, n\}$. On en déduit les inégalités $n \leqslant k$ et $k \leqslant n$, d'après le théorème précédent. Il s'ensuit $n = k$. ∎

**Définition**
Soit $E$ un ensemble fini. Si $E$ est non vide, le *cardinal* de $E$ est l'unique entier $n$ pour lequel il existe une bijection de $E$ sur $\{1, \ldots, n\}$. Si $E$ est vide, le *cardinal* de $E$ est égal à 0. Le cardinal de l'ensemble $E$ se note $\operatorname{Card} E$.

Il revient au même de dire que l'ensemble $E$ est de cardinal $n$ ou que l'ensemble $E$ a $n$ éléments.

**Proposition.** *Soient $E$ et $F$ des ensembles finis non vides. Il existe une bijection de $E$ sur $F$ si et seulement si on a $\operatorname{Card} E = \operatorname{Card} F$.*

**Démonstration.** Posons $n = \operatorname{Card} E$ et $k = \operatorname{Card} F$. Par définition, il existe des bijections $g : E \to \{1, \ldots, n\}$ et $h : F \to \{1, \ldots, k\}$. Supposons qu'il existe une bijection

$f : E \to F$. L'application $h \circ f$ est alors une bijection de $E$ sur $\{1, \ldots, k\}$. On en déduit $n = k$. Réciproquement, si $n = k$, alors $h^{-1} \circ g$ est une bijection de $E$ sur $F$. ∎

Si $E$ est un ensemble fini et si $A$ est une partie de $E$, alors intuitivement $A$ est un ensemble fini de cardinal inférieur ou égal au cardinal de $E$. Démontrons néanmoins ce résultat.

**Proposition.** *Soient $E$ un ensemble fini et $A$ une partie de $E$. Alors $A$ est un ensemble fini et l'on a $\operatorname{Card} A \leqslant \operatorname{Card} E$.*

**Démonstration.** Il suffit de faire la démonstration lorsque $E$ est l'ensemble $\{1, \ldots, n\}$, où $n$ est un entier positif. Soit $\mathscr{P}_n$ la propriété : toute partie de l'ensemble $\{1, \ldots, n\}$ est finie et de cardinal inférieur ou égal à $n$. La propriété $\mathscr{P}_1$ est vraie, car les parties de l'ensemble $\{1\}$ sont $\varnothing$ et $\{1\}$. Supposons que $n$ est un entier au moins égal à 2 et que la propriété $\mathscr{P}_{n-1}$ est vraie. Soit $A$ une partie de l'ensemble $\{1, \ldots, n\}$. Si $n \notin A$, alors $A$ est inclus dans l'ensemble $\{1, \ldots, n-1\}$. D'après l'hypothèse de récurrence, on en déduit que $A$ est finie et de cardinal inférieur ou égal à $n-1$. Supposons maintenant $n \in A$. L'ensemble $A' = A \setminus \{n\}$ est une partie de $E$ ne contenant pas $n$, donc, comme ci-dessus, on en déduit que $A'$ est un ensemble fini de cardinal inférieur ou égal à $n-1$. Il existe donc un entier $p \leqslant n-1$ et une bijection $f : A' \to \{1, \ldots, p\}$. Définissons la fonction $g : A \to \{1, \ldots, p+1\}$ en posant $g(x) = f(x)$ si $x \in A'$ et $g(n) = p+1$. Puisque $f$ est une bijection, $g$ est aussi une bijection. Par conséquent, $A$ est un ensemble fini de cardinal $p+1$ et puisqu'on a $p+1 \leqslant n$, cela montre que la propriété $\mathscr{P}_n$ est vraie. D'après le principe de récurrence, on en déduit que, pour tout $n$, la propriété $\mathscr{P}_n$ est vraie. ∎

Voici un résultat tout aussi intuitif et bien utile.

**Proposition.** *Si $A$ est une partie d'un ensemble fini $E$, on a l'équivalence*

$$A = E \iff \operatorname{Card} A = \operatorname{Card} E.$$

**Démonstration.** Si $A = E$, alors $\operatorname{Card} A = \operatorname{Card} E$. Montrons l'implication réciproque en raisonnant par contraposée, c'est-à-dire en démontrant que si $A$ est une partie de $E$ telle que $A \neq E$, alors $\operatorname{Card} A \neq \operatorname{Card} E$. Il suffit de considérer le cas $E = \{1, \ldots, n\}$, où $n$ est un entier positif. Soit $A$ une partie de $\{1, \ldots, n\}$ telle que $A \neq \{1, \ldots, n\}$. Si $n \notin A$, alors $A$ est une partie de l'ensemble $\{1, \ldots, n-1\}$. D'après la proposition précédente, on a alors $\operatorname{Card} A \leqslant n-1$ donc $\operatorname{Card} A < n$. Supposons que $n \in A$. Puisque $A$ n'est pas égal à $\{1, \ldots, n\}$, il existe un entier $p \in \{1, \ldots, n\}$ tel que $p \notin A$. Nécessairement, $p$ est différent de $n$. Posons $A' = (A \setminus \{n\}) \cup \{p\}$. L'application $f : A \to A'$ définie par $f(x) = x$ si $x \neq n$ et $f(n) = p$ est bijective. On a donc $\operatorname{Card} A = \operatorname{Card} A'$. Puisque $n \notin A'$, $A'$ est une partie de $\{1, \ldots, n-1\}$ donc $\operatorname{Card} A' \leqslant n-1$. On en déduit $\operatorname{Card} A < n$. ∎



**Formulaire sur les cardinaux.** Soit $E$ un ensemble fini.
Pour toutes parties $A$ et $B$ de $E$, on a

- $\operatorname{Card} A \leqslant \operatorname{Card} E$, $(A = E \Leftrightarrow \operatorname{Card} A = \operatorname{Card} E)$
- $\operatorname{Card}(A \cup B) = \operatorname{Card} A + \operatorname{Card} B$ si $A \cap B = \varnothing$
- et plus généralement $\operatorname{Card}(A \cup B) = \operatorname{Card} A + \operatorname{Card} B - \operatorname{Card}(A \cap B)$.

**Remarques**

- Si $E$ est un ensemble fini et si $A$ est une partie de $E$ telle que $A \neq E$, alors on a $\operatorname{Card} A < \operatorname{Card} E$ d'après le formulaire ci-dessus. Puisque deux ensembles en bijection ont même cardinal, on en déduit qu'il n'existe pas de bijection de $E$ sur $A$.
- Il n'en va pas de même lorsque l'ensemble $E$ est *infini*, c'est-à-dire n'est pas fini. Ainsi, il existe une application bijective de $\mathbb{N}$ sur $\mathbb{N} \setminus \{0\}$, par exemple l'application qui à tout entier naturel $n$ associe $n+1$.
  L'application $f : \mathbb{Z} \to \mathbb{N}$ définie par $f(n) = 2n$ pour tout entier naturel $n$ et $f(-n) = 2n - 1$ pour tout entier positif est également une bijection ; pourtant $\mathbb{N}$ est une partie de $\mathbb{Z}$ et $\mathbb{N}$ n'est pas égal à $\mathbb{Z}$.

**Cardinal d'un produit cartésien.** *Si $E$ et $F$ sont des ensembles finis, le produit cartésien $E \times F$ est un ensemble fini et l'on a $\operatorname{Card}(E \times F) = (\operatorname{Card} E)(\operatorname{Card} F)$.*

**Proposition.** *Soient $E$ et $F$ des ensembles finis non vides. Si $f : E \to F$ est une application, alors on a $\operatorname{Card} f(E) \leqslant \operatorname{Card} E$. De plus, on a $\operatorname{Card} f(E) = \operatorname{Card} E$ si et seulement si l'application $f$ est injective.*

**Démonstration.** Posons $n = \operatorname{Card} E$ et démontrons le résultat par récurrence sur $n$. Si $n = 1$, alors l'ensemble $E$ a un seul élément et donc l'ensemble $f(E)$ aussi. Dans ce cas, on a $\operatorname{Card} f(E) = 1$ et l'application $f$ est injective. Supposons $n \geqslant 2$ et la propriété démontrée pour l'entier $n-1$. Choisissons un élément $a$ de $E$ et posons $E' = E \setminus \{a\}$. Il vient $\operatorname{Card} E' = n - 1$. Soit $g : E' \to F$ l'application définie par $g(x) = f(x)$ pour tout $x \in E'$. On a $f(E) = \{f(a)\} \cup g(E')$, donc d'après le formulaire sur les cardinaux, il vient $\operatorname{Card} f(E) = \operatorname{Card} g(E')$ si $f(a) \in g(E')$ et $\operatorname{Card} f(E) = \operatorname{Card} g(E') + 1$ si $f(a) \notin g(E')$. Par hypothèse de récurrence, on a $\operatorname{Card} g(E') \leqslant n-1$ et $\operatorname{Card} g(E') = n-1$ si et seulement si l'application $g$ est injective. On en déduit $\operatorname{Card} f(E) \leqslant n$ et $\operatorname{Card} f(E) = n$ si et seulement si l'application $g$ est injective et $f(a) \notin g(E')$, c'est-à-dire si et seulement si l'application $f$ est injective. ∎

**Principe des tiroirs.** *Soient $E, F$ des ensembles finis non vides et $f : E \to F$ une application. Si $\operatorname{Card} E > \operatorname{Card} F$, alors il existe $a, b \in E$ tels que $a \neq b$ et $f(a) = f(b)$.*

**Démonstration.** Puisque $f(E)$ est une partie de $F$, on a $\operatorname{Card} f(E) \leqslant \operatorname{Card} F$. Puisque $\operatorname{Card} F < \operatorname{Card} E$, on en déduit l'inégalité $\operatorname{Card} f(E) < \operatorname{Card} E$. D'après la proposition précédente, l'application $f$ n'est pas injective, donc il existe des éléments $a, b \in E$ tels que $a \neq b$ et $f(a) = f(b)$. ∎

**Corollaire.** *Soient $E, F$ des ensembles finis non vides et $f : E \to F$ une application. Si $\operatorname{Card} F = \operatorname{Card} E$, alors les trois propriétés : $f$ est bijective, $f$ est injective et $f$ est surjective sont équivalentes.*

**Démonstration.** Puisqu'une application bijective est une application injective et surjective, il s'agit de montrer que l'application $f$ est injective si et seulement si elle est surjective. L'application $f$ est surjective si et seulement si $f(E) = F$, donc si et seulement si $\operatorname{Card} f(E) = \operatorname{Card} F$. Puisque $\operatorname{Card} F = \operatorname{Card} E$ par hypothèse, on en déduit que l'application $f$ est surjective si et seulement si $\operatorname{Card} f(E) = \operatorname{Card} E$. D'après la proposition précédente, cette dernière condition est équivalente à $f$ est injective. ∎

Terminons ce paragraphe en comptant le nombre d'applications d'un ensemble fini dans un autre, le nombre de parties d'un ensemble fini, le nombre de bijections d'un ensemble fini dans un autre de même cardinal et le nombre de parties à $p$ éléments d'un ensemble fini.

**Proposition.** *Si $E$ et $F$ sont des ensembles finis non vides, alors il y a $(\operatorname{Card} F)^{\operatorname{Card} E}$ applications de $E$ dans $F$.*

**Démonstration.** Posons $n = \operatorname{Card} E$, $k = \operatorname{Card} F$ et démontrons le résultat par récurrence sur $n$. Si l'ensemble $E$ n'a qu'un élément, alors le nombre d'applications de $E$ dans $F$ est le nombre d'images possibles pour cet élément, c'est-à-dire $k$. Supposons $n \geqslant 2$ et la propriété démontrée pour un ensemble de départ de cardinal $n-1$. Choisissons un élément $a$ de $E$ et posons $E' = E \setminus \{a\}$. Il vient $\operatorname{Card} E' = n-1$. Par hypothèse de récurrence, il y a $k^{n-1}$ applications de $E'$ dans $F$. Pour tout $y \in F$, il y a donc $k^{n-1}$ applications de $E$ dans $F$ telles que $f(a) = y$. On en déduit qu'il y a $k \times k^{n-1} = k^n$ applications de $E$ dans $F$. ∎

En particulier, si $E$ a $n$ éléments, alors il y a $n^n$ applications de $E$ dans $E$. Ainsi il y a 3125 applications de l'ensemble $\{1, 2, 3, 4, 5\}$ dans lui-même.

**Notation.** Pour tout entier positif $n$, on note $n!$ et on lit *factorielle* $n$ le produit des $n$ premiers entiers positifs. Ainsi l'on a $1! = 1$, $2! = 2$, $3! = 1 \times 2 \times 3 = 6$ et $4! = 1 \times 2 \times 3 \times 4 = 24$. Si $n$ est un entier supérieur ou égal à 2, l'entier $n!$ est égal à $1 \times 2 \times \cdots \times n$, ce qui se note aussi $1.2.\ldots.n$. Par convention, on pose $0! = 1$. Remarquons que pour tout entier positif $n$, on a $n! = (n-1)! \times n$.



**Proposition.** *Soit $n$ un entier positif. Si $E$ et $F$ sont des ensembles finis de cardinal $n$, alors il y a $n!$ bijections de $E$ sur $F$.*

**Démonstration.** On démontre le résultat par récurrence. Si $n = 1$, il y a une application de $E$ dans $F$ et cette application est bijective. Supposons $n \geqslant 2$ et la propriété démontrée pour des ensembles de cardinal $n-1$. Choisissons un élément $a$ de $E$. Pour tout $y \in F$, on a $\operatorname{Card}(E \setminus \{a\}) = \operatorname{Card}(F \setminus \{y\}) = n-1$, donc par hypothèse de récurrence il y a $(n-1)!$ bijections de $E \setminus \{a\}$ sur $F \setminus \{y\}$. On en déduit que pour tout $y \in F$, il y a $(n-1)!$ bijections $f$ de $E$ sur $F$ telles que $f(a) = y$. Il y a donc $n \times (n-1)! = n!$ bijections de $E$ sur $F$. ∎

En particulier, sur les 3125 applications de $\{1,2,3,4,5\}$ dans lui-même, 120 seulement sont bijectives.

**Proposition.** *Si $E$ est un ensemble fini non vide, alors il y a $2^{\operatorname{Card} E}$ parties de $E$.*

**Démonstration.** Posons $n = \operatorname{Card} E$ et démontrons le résultat par récurrence. Si $n = 1$, alors $E$ n'a qu'un élément et n'a que deux parties $\varnothing$ et $E$. Supposons $n \geqslant 2$ et la propriété démontrée pour tout ensemble de cardinal $n-1$. Choisissons un élément $a$ de $E$ et posons $E' = E \setminus \{a\}$. On a $\operatorname{Card} E' = n-1$ donc par hypothèse de récurrence, l'ensemble $E'$ a $2^{n-1}$ parties. Il y a deux sortes de parties de $E$ : celles qui contiennent $a$ et celles qui ne contiennent pas $a$. Une partie de $E$ qui ne contient pas $a$ est exactement une partie de $E'$, par suite il y a $2^{n-1}$ parties de $E$ qui ne contiennent pas $a$. Une partie de $E$ qui contient $a$ est la réunion de $\{a\}$ et d'une partie de $E'$. Il y a donc autant de parties de $E$ contenant $a$ que de parties ne contenant pas $a$, par suite il y a $2^{n-1} + 2^{n-1} = 2^n$ parties de $E$. ∎

### Nombre de parties à $p$ éléments d'un ensemble à $n$ éléments.

**Notation.** Si $n$ et $p$ sont des entiers naturels, notons $C_n^p$ le nombre de parties à $p$ éléments d'un ensemble à $n$ éléments.

Voici les premières propriétés de ces nombres.

- Dans un ensemble, il n'y a qu'une seule partie à 0 élément, l'ensemble vide ; on a donc $C_n^0 = 1$ pour tout entier naturel $n$. De plus, il y a autant de parties à un élément que d'éléments, donc $C_n^1 = n$.
- Soit $n$ un entier positif. Dans un ensemble $E$ à $n$ éléments, toute partie possède au plus $n$ éléments et la seule partie de $E$ à $n$ éléments est l'ensemble $E$ lui-même. On a donc $C_n^p = 0$ dès que $p > n$ et $C_n^n = 1$.

- Soit $n$ un entier positif. Puisqu'un ensemble à $n$ éléments a $2^n$ parties, on en déduit que l'on a $2^n = C_n^0 + \cdots + C_n^p + \cdots + C_n^n$.
- Soient $n$ un entier positif et $E$ un ensemble à $n$ éléments. Puisque le complémentaire d'une partie de $E$ à $p$ éléments est une partie à $n - p$ éléments, on en déduit que pour tout entier naturel $p$ tel que $p \leqslant n$, on a $C_n^{n-p} = C_n^p$.

**Proposition.** *Si $n$ et $p$ sont des entiers naturels tels que $0 < p < n$, alors on a*

$$C_n^p = C_{n-1}^p + C_{n-1}^{p-1}.$$

**Démonstration.** Soient $E$ un ensemble à $n$ éléments et $a$ un élément de $E$. Posons $E' = E \setminus \{a\}$. On a $\operatorname{Card} E' = n - 1$. Il y a deux sortes de parties de $E$ à $p$ éléments : celles qui contiennent $a$ et celles qui ne contiennent pas $a$. Une partie de $E$ à $p$ éléments qui ne contient pas $a$ est exactement une partie de $E'$ à $p$ éléments. Il s'ensuit qu'il y a $C_{n-1}^p$ parties de $E$ à $p$ éléments qui ne contiennent pas $a$. Une partie de $E$ à $p$ éléments qui contient $a$ est exactement la réunion de $\{a\}$ et d'une partie de $E'$ à $p - 1$ éléments. On en déduit qu'il y a $C_{n-1}^{p-1}$ parties de $E$ à $p$ éléments qui contiennent $a$. Il y a donc $C_{n-1}^p + C_{n-1}^{p-1}$ parties de $E$ à $p$ éléments. ∎

#### Triangle de Pascal

Voici une disposition commode pour calculer de proche en proche les entiers $C_n^p$. Puisque $C_n^p = 0$ si $p > n$, on a seulement à considérer les $C_n^p$ lorsque $0 \leqslant p \leqslant n$. Écrivons ces entiers de la manière suivante

$$\begin{array}{ccccccccccc}
 & & & & & C_0^0 & & & & & \\
 & & & & C_1^0 & & C_1^1 & & & & \\
 & & & C_2^0 & & C_2^1 & & C_2^2 & & & \\
 & & C_3^0 & & C_3^1 & & C_3^2 & & C_3^3 & & \\
 & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots \\
 & C_{n-1}^0 & & \cdots & C_{n-1}^{p-1} & & C_{n-1}^p & \cdots & & C_{n-1}^{n-1} & \\
C_n^0 & & C_n^1 & & \cdots & C_n^p & \cdots & & C_n^{n-1} & & C_n^n
\end{array}$$

où l'on fait figurer sur la $(n+1)$-ième ligne tous les entiers $C_n^p$ rangés selon les valeurs croissantes de $p$. Cette disposition s'appelle le *triangle de Pascal*.

Puisque $C_n^0 = C_n^n = 1$ pour tout entier naturel $n$, on en déduit qu'aux extrémités de toutes les lignes du triangle de Pascal figurent des 1. Puisqu'on a $C_n^1 = n$, il vient $C_2^1 = 2$, $C_3^1 = 3$ et $C_4^1 = 4$. On en déduit $C_3^2 = 3$ et $C_4^3 = 4$. D'après la proposition précédente, on a $C_4^2 = C_3^2 + C_3^1 = 3 + 3 = 6$.

Plus généralement, si l'on a calculé la $n$-ième ligne, c'est-à-dire tous les $C_{n-1}^p$, la $(n+1)$-ième ligne se remplit en utilisant la règle de formation donnée dans la proposition précédente. De plus, puisqu'on a $C_n^p = C_n^{n-p}$, chaque ligne est symétrique par rapport à son milieu. Voici par exemple le triangle de Pascal jusqu'à l'entier $n = 5$.

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1
\end{array}$$

Lorsqu'on a besoin d'une formule générale pour les entiers $C_n^p$, on utilise la proposition suivante.

**Proposition.** *Si $n$ et $p$ sont des entiers naturels tels que $p \leqslant n$, alors on a*

$$C_n^p = \frac{n!}{p!(n-p)!}.$$

**Démonstration.** Pour tout entier naturel $n$, soit la propriété $\mathscr{P}_n$ : pour tout entier naturel $p$ tel que $p \leqslant n$, on a $C_n^p = \dfrac{n!}{p!(n-p)!}$.

Rappelons que par convention, on pose $0! = 1$. Puisqu'on a $C_0^0 = C_1^0 = C_1^1 = 1$, les propriétés $\mathscr{P}_0$ et $\mathscr{P}_1$ sont vraies.

Soit $n$ un entier supérieur ou égal à 2. Supposons la propriété $\mathscr{P}_{n-1}$ vraie. Soit $p$ un entier naturel tel que $p \leqslant n$. Si l'entier $p$ est égal à 0 ou à $n$, on a $C_n^p = 1$ et $\dfrac{n!}{p!(n-p)!} = \dfrac{n!}{n!} = 1$, donc la formule est vraie. Supposons $0 < p < n$. D'après la proposition précédente, on a $C_n^p = C_{n-1}^p + C_{n-1}^{p-1}$. Par hypothèse de récurrence, il vient $C_{n-1}^p = \dfrac{(n-1)!}{p!(n-1-p)!}$ et $C_{n-1}^{p-1} = \dfrac{(n-1)!}{(p-1)!(n-p)!}$. On en déduit les égalités

$$\begin{aligned}
C_n^p &= \frac{(n-1)!}{p!(n-1-p)!} + \frac{(n-1)!}{(p-1)!(n-p)!} = \frac{(n-1)!}{p!(n-p)!}\left((n-p)+p\right) \\
&= \frac{(n-1)!}{p!(n-p)!}\,n = \frac{n!}{p!(n-p)!}
\end{aligned}$$

d'où la propriété $\mathscr{P}_n$. On a donc démontré par récurrence que la propriété $\mathscr{P}_n$ est vraie quel que soit l'entier naturel $n$. ∎

## Exercices

**1.** On considère les ensembles

$$E = \left\{ x \in [0,1] \mid \exists n \in \mathbb{N},\ x < \frac{1}{n+1} \right\} \quad \text{et} \quad F = \left\{ x \in [0,1] \mid \forall n \in \mathbb{N},\ x < \frac{1}{n+1} \right\}.$$

**a)** L'ensemble $E$ a-t-il un, une infinité ou aucun élément ?

**b)** L'ensemble $F$ a-t-il un, une infinité ou aucun élément ?

**2.** Soit l'application $f : \mathbb{R}^2 \to \mathbb{R}^2$ définie par $f(x,y) = (x+y, 2x+3y)$ pour tous $x, y \in \mathbb{R}$. Montrer que l'application $f$ est bijective.

**3.** Soit l'application $f : \mathbb{R}^2 \to \mathbb{R}^2$ définie par $f(x,y) = (2x-3y, -4x+6y)$ pour tous $x, y \in \mathbb{R}$.

**a)** L'ensemble $\{ (x,y) \in \mathbb{R}^2 \mid f(x,y) = (0,0) \}$ a-t-il un, une infinité ou aucun élément ?

**b)** Montrer que l'application $f$ n'est pas injective.

**c)** Posons $B = \{ (x,y) \in \mathbb{R}^2 \mid 2x + y = 0 \}$. Montrer l'égalité $f(\mathbb{R}^2) = B$.

**4.** Soient les applications $f : \mathbb{R} \to \mathbb{R}$ et $g : \mathbb{R} \to \mathbb{R}$ définies par $f(x) = \frac{1}{2}x(x-1)$ et $g(x) = f(x+1)$ pour tout $x \in \mathbb{R}$.

**a)** L'application $f$ est-elle injective ?

**b)** Montrer que l'application $f$ n'est pas surjective.

**c)** Montrer que l'on a $g(\mathbb{N}) = f(\mathbb{N})$.

**5.** Soit l'application $f : \mathbb{R}^2 \to \mathbb{R}$ définie par $f(x,y) = x - y^2$ pour tous $x, y \in \mathbb{R}$.

**a)** L'application $f$ est-elle injective ?

**b)** Montrer que l'application $f$ est surjective.

**c)** Trouver une application $g : \mathbb{R} \to \mathbb{R}^2$ telle que $f \circ g = \mathrm{id}_{\mathbb{R}}$.

**d)** Soit l'application $h : \mathbb{R}^2 \to \mathbb{R}^2$ définie par $h(x,y) = (x+y^2, y)$ pour tous $x, y \in \mathbb{R}$. Montrer que $h$ est une bijection. Calculer $f \circ h(x,y)$ pour tous $x, y \in \mathbb{R}$.

**6.** Soit $f : \mathbb{R} \to \mathbb{R}$ une application. On suppose que pour tous nombres réels $x, y$ tels que $x < y$, on a $f(x) < f(y)$. Montrer que l'application $f$ est injective.

**7.** Soient $E$, $F$, $G$ des ensembles et $f : E \to F$, $g : F \to G$ des applications.

**a)** Montrer que si les applications $f$ et $g$ sont injectives, alors l'application $g \circ f$ est injective.

**b)** Montrer que si les applications $f$ et $g$ sont surjectives, alors l'application $g \circ f$ est surjective.

**c)** Montrer que si l'application $g \circ f$ est injective, alors l'application $f$ est injective.

**d)** Montrer que si l'application $g \circ f$ est surjective, alors l'application $g$ est surjective.



**8.** Soient $E$, $F$, $G$ des ensembles et $f : E \to F$, $g : F \to G$, $h : G \to E$ des applications. On suppose que l'application $h \circ g \circ f$ est surjective et que les applications $g \circ f \circ h$ et $f \circ h \circ g$ sont injectives.

**a)** Montrer que l'application $h$ est injective et surjective.

**b)** Montrer que l'application $g \circ f$ est bijective.

**c)** Montrer que $f$, $g$ et $h$ sont des bijections.

**9.** Soient $E$ un ensemble non vide et $f : E \to \mathscr{P}(E)$ une application.

**a)** Posons $A = \{ x \in E \mid x \notin f(x) \}$. Soit $x \in E$. Montrer que $x \in f(x) \cup A$ et que $x \notin f(x) \cap A$. En déduire $f(x) \neq A$.

**b)** Montrer que l'application $f$ n'est pas surjective.

**10.** Soit l'application $f : \mathbb{N}^2 \to \mathbb{N}$ définie par $f(n,k) = \frac{1}{2}(n+k)(n+k+1)+k$ pour tous $n, k \in \mathbb{N}$.

**a)** Soient $n$, $k$, $n'$ et $k'$ des entiers naturels tels que $n + k > n' + k'$. Démontrer l'inégalité $f(n,k) \geqslant f(n',k') + n' + k + 1$.

**b)** Montrer que l'application $f$ est injective.

**c)** Soit $p \in \mathbb{N}$. Montrer qu'il existe $a \in \mathbb{N}$ tel que $\frac{1}{2}a(a+1) \leqslant p < \frac{1}{2}(a+1)(a+2)$.

**d)** Soient $n$ et $k$ des entiers naturels tels que $0 \leqslant k \leqslant n$. Calculer $f(n-k, k)$.

**e)** Montrer que l'application $f$ est bijective.

**11.** Soit $E$ un ensemble fini de cardinal $n \geqslant 1$. Notons $F$ l'ensemble des applications de $E$ dans $\{0,1\}$.

**a)** Quel est le cardinal de $F$ ?

**b)** Pour toute partie $A$ de $E$, notons $C_A$ la fonction de $E$ dans $\{0,1\}$ définie par $C_A(x) = 1$ si $x \in A$ et $C_A(x) = 0$ si $x \notin A$. Soit $\varphi$ l'application de $\mathscr{P}(E)$ dans $F$ qui à toute partie $A$ de $E$ associe $C_A$. Montrer que $\varphi$ est une application injective. En déduire que l'application $\varphi$ est bijective.

**12.** Soient $n$ un entier au moins égal à 2 et $E$ un ensemble à $n$ éléments. Soit $f : E \to \mathscr{P}(E)$ une application. On suppose que pour tout $x \in E$, on a $x \in f(x)$ et que pour tous $x, y \in E$, on a l'implication $x \in f(y) \Rightarrow y \in f(x)$.

**a)** Montrer que pour tout $x \in E$, on a $\mathrm{Card}\, f(x) \geqslant 1$.

**b)** On suppose qu'il existe $a \in E$ tel que $\mathrm{Card}\, f(a) = n$. Montrer que pour tout $x \in E$, on a $\mathrm{Card}\, f(x) \geqslant 2$.

**c)** Montrer qu'il existe des éléments $x, y \in E$ différents tels que les ensembles $f(x)$ et $f(y)$ aient le même nombre d'éléments.

**13.** L'ensemble $\{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid x^2 - y^2 = 15\}$ est-il fini ?

**14.** Soit $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ l'application définie par $f(x, y) = x^2 - 2xy + 3y^2$ pour tous entiers relatifs $x$ et $y$. Soit $n$ un entier relatif.

**a)** Supposons $n < 0$. Montrer que l'ensemble $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid f(x, y) = n\}$ est vide.

**b)** Supposons $n \geqslant 0$. L'ensemble $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid f(x, y) = n\}$ est-il fini ?

## Quelques réponses ou indications

1. On a $E = ]0, 1[$ et $F = \{0\}$.

2. Chercher $x$ et $y$ en fonction de $a$ et $b$ tels que $f(x, y) = (a, b)$.

3. **a)** Une infinité : pour tout $x \in \mathbb{R}$, on a $f(3x, 2x) = (0, 0)$.

 **c)** Ne pas oublier de démontrer l'inclusion $B \subset f(\mathbb{R}^2)$. Pour cela il faut, quel que soit $(x, y) \in B$, chercher des nombres réels $a$ et $b$ tels que $f(a, b) = (x, y)$.

4. **a)** Non.

 **b)** Trouver une condition sur $y \in \mathbb{R}$ pour qu'il existe $x \in \mathbb{R}$ tel que $f(x) = y$.

 **c)** Pour tout $n \in \mathbb{N}$, on a $g(n) = f(n + 1)$ donc $g(n) \in f(\mathbb{N})$. Il s'ensuit $g(\mathbb{N}) \subset f(\mathbb{N})$. D'autre part on a $f(0) = 0 = f(1) = g(0)$, par suite $f(0) \in g(\mathbb{N})$. Si $n$ est un entier positif, il vient $f(n) = g(n - 1)$, donc $f(n) \in g(\mathbb{N})$. On en déduit l'inclusion $f(\mathbb{N}) \subset g(\mathbb{N})$.

5. **a)** Non.

 **c)** Par exemple $g(x) = (x, 0)$.

8. **a)** Puisque l'application $(g \circ f) \circ h$ est injective, l'application $h$ l'est aussi, d'après **(c)** de l'exercice 7. Puisque l'application $h \circ (g \circ f)$ est surjective, l'application $h$ l'est aussi, d'après **(d)** de l'exercice 7.

10. **a)** Utiliser l'inégalité $n + k \geqslant n' + k' + 1$.

 **b)** Si $f(n, k) = f(n', k')$, utiliser **(a)** pour démontrer que $n + k = n' + k'$.

 **e)** Soit $p \in \mathbb{N}$. D'après **(c)**, il existe $a \in \mathbb{N}$ tel que $\frac{1}{2}a(a+1) \leqslant p < \frac{1}{2}(a+1)(a+2)$. Si $b = p - \frac{1}{2}a(a+1)$, montrer que $b \leqslant a$ et calculer $f(a - b, b)$.

12. **b)** Puisque $f(a)$ est une partie de $E$ telle que $\operatorname{Card} f(a) = \operatorname{Card} E$, on a $f(a) = E$. En déduire que $a \in f(x)$ quel que soit $x \in E$. Si $x \neq a$, on a donc $\{a, x\} \subset f(x)$.

 **c)** Puisqu'on a $1 \leqslant \operatorname{Card} f(x) \leqslant n$ quel que soit $x \in E$, on définit une application $g : E \to \{1, 2, \ldots, n\}$ en posant $g(x) = \operatorname{Card} f(x)$. Il s'agit de montrer que $g$ n'est pas injective. Pour cela, montrer que l'application $g$ n'est pas surjective en utilisant **(b)**.

13. Cet ensemble possède huit éléments.

14. **a)** On a $f(x, y) = (x - y)^2 + 2y^2$.

 **b)** Soit $(x, y) \in \mathbb{Z} \times \mathbb{Z}$. Si l'on a $f(x, y) = n$, alors les entiers $2y^2$ et $(x - y)^2$ sont inférieurs ou égaux à $n$.





# Chapitre 3

# Les nombres complexes

Il n'existe pas de nombre réel $x$ tel que $x^2 = -1$. Nous allons introduire de nouveaux nombres, les *nombres complexes*, de manière à donner des solutions non seulement à cette équation, mais encore à bien d'autres.

## 1. Règles de calcul

Un nombre complexe s'écrit de manière unique $a + bi$, où $a$ et $b$ sont des nombres réels. De manière unique, cela veut dire que si $a, b, c, d$ sont des nombres réels tels que $a + bi = c + di$, alors on a $a = c$ et $b = d$. L'ensemble des nombres complexes se note $\mathbb{C}$.

**Définitions**

Soit $z$ un nombre complexe. Soient $a$ et $b$ les nombres réels tels que $z = a + bi$. Le nombre $a$ s'appelle la *partie réelle* de $z$ et se note $\mathcal{Re}\, z$. Le nombre $b$ s'appelle la *partie imaginaire* de $z$ et se note $\mathcal{Im}\, z$.

On définit les opérations somme et produit des nombres complexes $a + bi$ et $c + di$ de la manière suivante :

- $(a + bi) + (c + di) = (a + c) + (b + d)i$
- $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$.

En utilisant les règles de calcul sur les nombres réels, une simple vérification montre que pour tous nombres complexes $z$, $z'$ et $z''$ on a :

- $z + z' = z' + z$, $\mathcal{Re}(z + z') = \mathcal{Re}\, z + \mathcal{Re}\, z'$, $\mathcal{Im}(z + z') = \mathcal{Im}\, z + \mathcal{Im}\, z'$
- $(z + z') + z'' = z + (z' + z'')$ et ce nombre complexe est noté $z + z' + z''$
- $zz' = z'z$, $z(z' + z'') = zz' + zz''$
- $(zz')z'' = z(z'z'')$ et ce nombre complexe est noté $zz'z''$.

Faisons une première convention. Si $a$ est un nombre réel, notons simplement $a$ le nombre complexe $a+0i$ ; cela est légitime car les opérations sur les nombres complexes de la forme $a+0i$ sont les mêmes que les opérations sur les nombres réels. Avec cette convention, on en déduit que pour tout nombre complexe $z$ et pour tout nombre réel $\lambda$, on a :

- $z=0 \Leftrightarrow \mathcal{R}e\, z = \mathcal{I}m\, z = 0$
- $\mathcal{R}e(\lambda z) = \lambda \mathcal{R}e\, z, \quad \mathcal{I}m(\lambda z) = \lambda \mathcal{I}m\, z$
- $z+0=z, \quad 1z=z, \quad 0z=0.$

**Notation.** Si $z$ est le nombre complexe $a+bi$, notons $-z$ le nombre complexe $-a+(-b)i$. De plus, si $z'$ est un autre nombre complexe, notons $z'-z$ le nombre complexe $z'+(-z)$.

Pour tout nombre complexe $z$, on a alors $z-z=0$.

Une seconde convention consiste à noter simplement $i$ le nombre complexe $0+1i$. Si $a$ et $b$ sont des nombres réels, nous pouvons maintenant faire le produit $bi$ des nombres complexes $b$ et $i$ ; la somme des nombres complexes $a$ et $bi$ est bien alors le nombre complexe $a+bi$. C'est cette cohérence qui justifie la convention que nous venons de faire. Calculons par exemple le produit de $i$ par lui-même, que l'on note $i^2$. Il vient $i^2=(0+1i)(0+1i)=-1+0i$ donc nous avons la formule importante

$$i^2=-1.$$

Ainsi le nombre complexe $i$ est solution de l'équation $x^2=-1$.

**Proposition.** *Soit $z$ un nombre complexe tel que $z \neq 0$. Il existe un unique nombre complexe $z'$, noté $1/z$ ou bien $\frac{1}{z}$, tel $zz'=1$. De plus, si $z=a+bi$ où $a,b \in \mathbb{R}$, alors on a*

$$\frac{1}{z} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}\, i\,.$$

**Démonstration.** Écrivons $z=a+bi$ avec $\mathcal{R}e\, z=a$ et $\mathcal{I}m\, z=b$ et démontrons qu'il existe des nombres réels $a'$ et $b'$ uniques tels que $(a+bi)(a'+b'i)=1$. Puisque $z$ est non nul, on a $(a,b)\neq(0,0)$, autrement dit les nombres réels $a$ et $b$ ne sont pas tous les deux nuls. Par suite le nombre réel $a^2+b^2$ est strictement positif, donc non nul. D'autre part, pour tous nombres réels $a'$ et $b'$, il vient

$$(a+bi)(a'+b'i)=1 \iff (aa'-bb')+(ba'+ab')i=1$$
$$\iff \begin{cases} aa'-bb'=1 \\ ba'+ab'=0. \end{cases}$$

Multiplions la première égalité par $a$, la seconde par $b$ et ajoutons-les ; nous obtenons $(a^2+b^2)a'=a$. De même, en multipliant la première égalité par $-b$ et la seconde par $a$, on obtient $(a^2+b^2)b'=-b$. Il vient $a'=\frac{a}{a^2+b^2}$, $b'=\frac{-b}{a^2+b^2}$ et l'on vérifie que l'on a bien $(a+bi)(a'+b'i)=1$. ∎



**Corollaire.** *Soient $z$ et $z'$ des nombres complexes. On a l'équivalence*

$$zz'=0 \iff (z=0 \text{ ou } z'=0)\,.$$

**Démonstration.** Si par exemple $z=0$, alors nous savons déjà que $zz'=0z'=0$. Supposons $zz'=0$ et $z\neq 0$. Il vient $z'=1z'=\big((1/z)z\big)z'=(1/z)(zz')=(1/z)0=0$. ∎

**Notations.** Si $z$ et $z'$ sont des nombres complexes et si $z'\neq 0$, le produit de $z$ par $1/z'$ se note $z/z'$, ou bien $\frac{z}{z'}$.

Pour tout nombre complexe $z$, on pose $z^0=1$ et si $n$ est un entier positif on note $z^n$ le produit de $z^{n-1}$ par $z$.

Pour tous entiers naturels $n$ et $p$ et pour tout nombre complexe $z$, on a

$$z^n z^p = z^{n+p} \quad \text{et} \quad (z^n)^p = z^{np}\,.$$

**Exemple.** La formule $i^2=-1$ permet de calculer toutes les puissances de $i$. En effet, pour tout entier naturel $n$, on a $i^{2n}=(i^2)^n=(-1)^n$ et $i^{2n+1}=i^{2n}i=(-1)^n i$. Il vient donc

$$i^{4n}=1\,, \quad i^{4n+1}=i\,, \quad i^{4n+2}=-1\,, \quad i^{4n+3}=-i\,.$$

**Définitions**

Soient $z$ un nombre complexe et $n$ un entier supérieur ou égal à 2. Le nombre complexe $z^n$ s'appelle la *puissance $n$-ième* de $z$ et plus simplement le carré de $z$ lorsque $n=2$, le cube lorsque $n=3$. Si l'on a $z^n=\alpha$ on dit que $z$ est une *racine $n$-ième* de $\alpha$ et plus simplement une racine carrée de $\alpha$ lorsque $n=2$, une racine cubique lorsque $n=3$.

Remarquons que si $z$ et $z'$ sont des nombres complexes, on a les équivalences

$$z^2=z'^2 \iff (z-z')(z+z')=0 \iff z=\pm z'\,.$$

Il s'ensuit que tout nombre complexe a au plus deux racines carrés.

**Exemple.** Si $a$ est un nombre réel non nul, alors les racines carrées de $a$ sont $\sqrt{a}$ et $-\sqrt{a}$ si $a>0$ et les nombres complexes $i\sqrt{-a}$ et $-i\sqrt{-a}$ si $a<0$.

**Proposition.** *Pour tout nombre complexe $z$ différent de 1 et pour tout entier positif $n$, on a*

$$1 + z + \cdots + z^n = \frac{1 - z^{n+1}}{1 - z}.$$

**Démonstration.** Soit $z$ un nombre complexe différent de 1. Pour tout entier positif $n$, posons $S_n = 1 + z + \cdots + z^n$. Démontrons par récurrence que l'on a $(1-z)S_n = 1 - z^{n+1}$, ce qui permettra de conclure, car le nombre complexe $1 - z$ n'est pas nul. On a $(1-z)S_1 = (1-z)(1+z) = 1 - z^2$, donc la propriété est vraie pour l'entier 1. Soit $n$ un entier supérieur ou égal à 2. Supposons la propriété vraie pour l'entier $n-1$. Par définition, on a $S_n = S_{n-1} + z^n$. On en déduit les égalités $(1-z)S_n = (1-z)S_{n-1} + (1-z)z^n = (1-z)S_{n-1} + z^n - z^{n+1}$. D'après l'hypothèse de récurrence, on a $(1-z)S_{n-1} = 1 - z^n$. Par conséquent il vient $(1-z)S_n = 1 - z^n + z^n - z^{n+1} = 1 - z^{n+1}$, ce qu'il fallait démontrer. ∎

Rappelons qu'au précédent chapitre nous avons introduit, pour tous entiers naturels $n$ et $p$, l'entier $C_n^p$ et que nous avons démontré l'égalité $C_n^p = \dfrac{n!}{p!(n-p)!}$ si $p \leqslant n$.

**Formule du binôme de Newton.** *Pour tous nombres complexes $z$ et $z'$ et pour tout entier $n$ supérieur ou égal à 2, on a*

$$(z + z')^n = z^n + C_n^1 z^{n-1} z' + \cdots + C_n^k z^{n-k} z'^k + \cdots + C_n^{n-1} z z'^{n-1} + z'^n.$$

**Démonstration.** La formule se démontre par récurrence. Il vient $(z + z')^2 = z^2 + 2zz' + z'^2$. Puisqu'on a $C_2^1 = 2$, la formule est vraie si $n = 2$. Soit $n$ un entier supérieur ou égal à 3. Supposons la formule vraie pour l'entier $n - 1$, c'est-à-dire que l'on a $(z + z')^{n-1} = z^{n-1} + \cdots + C_{n-1}^p z^{n-1-p} z'^p + \cdots + z'^{n-1}$. On en déduit

$$\begin{aligned}
(z + z')^n &= (z + z')(z + z')^{n-1} = z(z + z')^{n-1} + z'(z + z')^{n-1} \\
&= z\left(z^{n-1} + \cdots + C_{n-1}^k z^{n-1-k} z'^k + \cdots + z'^{n-1}\right) + \\
&\qquad z'\left(z^{n-1} + \cdots + C_{n-1}^{k-1} z^{(n-1)-(k-1)} z'^{k-1} + \cdots + z'^{n-1}\right) \\
&= z^n + \cdots + \left(C_{n-1}^k + C_{n-1}^{k-1}\right) z^{n-k} z'^k + \cdots + z'^n.
\end{aligned}$$

Or nous avons démontré page 28 que l'on a l'égalité $C_{n-1}^k + C_{n-1}^{k-1} = C_n^k$ pour tout entier $k$ tel que $1 \leqslant k \leqslant n - 1$. Il s'ensuit $(z + z')^n = z^n + \cdots + C_n^k z^{n-k} z'^k + \cdots + z'^n$, ce qu'il fallait démontrer. ∎

Cette proposition justifie la définition suivante.

**Définition**

Si $n$ et $p$ sont des entiers naturels tels que $p \leqslant n$, les entiers $C_n^p$ s'appellent les *coefficients binômiaux*.





Rappelez-vous : pour calculer les coefficients binômiaux $C_n^p$ pour des petites valeurs de $n$, il est commode d'utiliser le triangle de Pascal.

## 2. Conjugué et module d'un nombre complexe

**Définitions**

Soit $z$ un nombre complexe. Posons $a = \mathcal{R}e\, z$ et $b = \mathcal{I}m\, z$.

- Le nombre complexe $a - bi$ s'appelle le *conjugué* de $z$ et se note $\bar{z}$.
- Le nombre réel $\sqrt{a^2 + b^2}$ s'appelle le *module* de $z$ et se note $|z|$.

**Remarques**

- Le module d'un nombre complexe est un nombre réel positif ou nul.
- Pour tout nombre réel $a$, $\sqrt{a^2}$ est égal à la valeur absolue de $a$ : le module des nombres complexes prolonge la valeur absolue des nombres réels.

| Formulaire |
|---|
| $\bar{\bar{z}} = z$ $\quad$ $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ $\quad$ $\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$ $\quad$ $\overline{1/z} = 1/\bar{z}$ |
| $\mathcal{R}e\, z = \frac{1}{2}(z + \bar{z})$ $\quad$ $\mathcal{I}m\, z = \frac{1}{2i}(z - \bar{z})$ |
| $z \in \mathbf{R} \iff \bar{z} = z$ $\quad$ $z \in \mathbf{R}i \iff iz \in \mathbf{R} \iff \bar{z} = -z$ |
| $\lvert z\rvert^2 = z\bar{z}$ $\quad$ $\lvert\bar{z}\rvert = \lvert z\rvert$ $\quad$ $\lvert zz'\rvert = \lvert z\rvert\,\lvert z'\rvert$ $\quad$ $\lvert 1/z\rvert = 1/\lvert z\rvert$ |
| $\left(z = 0 \Leftrightarrow \lvert z\rvert = 0\right)$ $\quad$ $\left(z \neq 0 \Rightarrow \frac{1}{z} = \frac{\bar{z}}{\lvert z\rvert^2}\right)$ $\quad$ $\left(\lvert z\rvert = 1 \Rightarrow \frac{1}{z} = \bar{z}\right)$ |
| $\lvert z + z'\rvert^2 = \lvert z\rvert^2 + 2\,\mathcal{R}e(z'\bar{z}) + \lvert z'\rvert^2$ |

Contentons-nous de démontrer quelques-unes de ces formules.

- Si $z_1 = a_1 + b_1 i$ et $z_2 = a_2 + b_2 i$, alors on a $z_1 z_2 = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)i$ et $\overline{z_1}\,\overline{z_2} = (a_1 - b_1 i)(a_2 - b_2 i) = (a_1 a_2 - b_1 b_2) - (a_1 b_2 + a_2 b_1)i$. Il s'ensuit $\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$.
- Si $z = a + bi$, il vient $z\bar{z} = (a + bi)(a - bi) = a^2 + b^2 = |z|^2$.

- Soient $z$ et $z'$ des nombres complexes. D'après ce que nous venons de démontrer, on a $|zz'|^2 = zz'\overline{zz'}$ et $|z|^2|z'|^2 = z\bar{z}z'\bar{z'}$, donc $|zz'|^2 = (|z|\,|z'|)^2$. Puisque le module d'un nombre complexe est un nombre réel positif ou nul, il vient $|zz'| = |z|\,|z'|$.
- Enfin, démontrons la dernière formule. Nous avons

$$\begin{aligned}|z+z'|^2 &= (z+z')(\overline{z+z'}) = (z+z')(\bar{z}+\bar{z'}) = z\bar{z} + z'\bar{z} + z\bar{z'} + z'\bar{z'}\\ &= |z|^2 + z'\bar{z} + \overline{z'\bar{z}} + |z'|^2 = |z|^2 + 2\,\mathcal{R}e\,(z'\bar{z}) + |z'|^2.\end{aligned}$$

Pour calculer la partie réelle et la partie imaginaire d'un nombre complexe de la forme $z'/z$, on multiplie le numérateur et le dénominateur par le conjugué de $z$, ce qui donne $z'/z = z'\bar{z}/|z|^2$. Dans cette dernière expression, le dénominateur est un nombre réel.

**Exemple.** Supposons $z \in \mathbb{C}$, $z \neq 1/2$ et posons $z' = \dfrac{2z+1}{2z-1}$. On a

$$z' = \frac{(2z+1)\,(\overline{2z-1})}{|2z-1|^2} = \frac{(2z+1)\,(2\bar{z}-1)}{|2z-1|^2} = \frac{4|z|^2-1}{|2z-1|^2} - 2\,\frac{z-\bar{z}}{|2z-1|^2}\,.$$

Puisque $4|z|^2 - 1$ est un nombre réel et puisque $z - \bar{z} = 2i\,\mathcal{I}m\,z$, on en déduit

$$\mathcal{R}e\,z' = \frac{4|z|^2-1}{|2z-1|^2} \quad \text{et} \quad \mathcal{I}m\,z' = -\,\frac{4\,\mathcal{I}m\,z}{|2z-1|^2}\,.$$

**Remarque**
Soient $a,b,c,d$ des nombres réels. D'après la formule sur le module d'un produit, on a l'égalité $|(a+bi)(c+di)|^2 = |a+bi|^2|c+di|^2$. Puisque $(a+bi)(c+di) = (ac-bd)+(ad+bc)i$, on en déduit l'identité

$$(ac-bd)^2 + (ad+bc)^2 = (a^2+b^2)(c^2+d^2)\,.$$

Cette identité est intéressante lorsqu'on l'applique à des nombres entiers $a,b,c,d$ :
- un entier de la forme $x^2+y^2$, où $x$ et $y$ sont des entiers, s'appelle "une somme de deux carrés" ; par exemple, $5 = 1^2+2^2$, $13 = 2^2+3^2$ et $41 = 4^2+5^2$ sont des sommes de deux carrés, mais 7, 11 et 19 n'en sont pas.
- Si $a,b,c,d$ sont des entiers quelconques, le membre de droite de l'identité est le produit de deux entiers qui sont chacun une somme de deux carrés ; le membre de gauche étant une somme de deux carrés, on a le résultat suivant :
le produit de deux entiers qui sont sommes de deux carrés est une somme de deux carrés.

**Lemme.** *Pour tout nombre complexe $z$, on a $|\mathcal{R}e\,z| \leqslant |z|$ et $|\mathcal{I}m\,z| \leqslant |z|$.*

**Démonstration.** Soit $z$ un nombre complexe. Posons $a = \mathcal{R}e\,z$ et $b = \mathcal{I}m\,z$. On a les inégalités $a^2 \leqslant a^2+b^2$ et $b^2 \leqslant a^2+b^2$. La fonction racine carrée étant croissante, on en déduit les inégalités $\sqrt{a^2} \leqslant \sqrt{a^2+b^2}$ et $\sqrt{b^2} \leqslant \sqrt{a^2+b^2}$, c'est-à-dire $|a| \leqslant \sqrt{a^2+b^2}$ et $|b| \leqslant \sqrt{a^2+b^2}$, ce qu'il fallait démontrer. ■





**Inégalité triangulaire.** *Pour tous nombres complexes $z, z'$, on a $|z+z'| \leqslant |z| + |z'|$.*

**Démonstration.** Soient $z$ et $z'$ des nombres complexes. Puisque $|z+z'|$ est un nombre réel positif ou nul, on a $|z+z'| \leqslant |z|+|z'|$ si et seulement si $|z+z'|^2 \leqslant (|z|+|z'|)^2$. Calculons la différence $(|z|+|z'|)^2 - |z+z'|^2$. Il vient

$$\begin{aligned}(|z|+|z'|)^2 - |z+z'|^2 &= |z|^2 + 2|z|\,|z'| + |z'|^2 - (|z|^2 + 2\,\mathcal{R}e\,(z'\bar{z}) + |z'|^2)\\ &= 2(|\bar{z}|\,|z'| - \mathcal{R}e\,(z'\bar{z}))\\ &= 2(|z'\bar{z}| - \mathcal{R}e\,(z'\bar{z})).\end{aligned}$$

D'après le lemme précédent, la différence $|z'\bar{z}| - \mathcal{R}e\,(z'\bar{z})$ est positive ou nulle. On en déduit l'inégalité $(|z|+|z'|)^2 - |z+z'|^2 \geqslant 0$, ce qu'il fallait démontrer. ■

**Corollaire.** *Pour tous nombres complexes $z, z'$, on a $\big||z| - |z'|\big| \leqslant |z - z'|$.*

**Démonstration.** Soient $z$ et $z'$ des nombres complexes. On a $z = (z-z')+z'$. D'après l'inégalité triangulaire, il vient $|z| \leqslant |z-z'|+|z'|$, c'est-à-dire $|z|-|z'| \leqslant |z-z'|$. De même on a $z' = (z'-z)+z$ et l'inégalité $|z'|-|z| \leqslant |z'-z|$. Puisque $z'-z = -(z-z')$, on a $|z'-z| = |-1|\,|z-z'| = |z-z'|$. On a ainsi démontré que $|z|-|z'| \leqslant |z-z'|$ et $-(|z|-|z'|) \leqslant |z-z'|$, d'où le résultat. ■

**Racines carrées d'un nombre complexe.** Nous avons vu que tout nombre réel non nul possède deux racines carrées opposées. Plus généralement, nous allons montrer que tout nombre complexe non nul possède aussi deux racines carrées opposées que l'on peut calculer explicitement.

**Proposition.** *Soient $a$ et $b$ des nombres réels. Supposons $b \neq 0$ et posons $\varepsilon = 1$ si $b > 0$ et $\varepsilon = -1$ si $b < 0$. Les racines carrées de $a+bi$ sont les nombres complexes*

$$z = \frac{1}{\sqrt{2}}\left(\sqrt{\sqrt{a^2+b^2}+a} + i\,\varepsilon\sqrt{\sqrt{a^2+b^2}-a}\right) \quad \text{et} \quad -z\,.$$

**Démonstration.** Soient $x$ et $y$ des nombres réels. Puisque $(x+yi)^2 = x^2-y^2+2xyi$, on a l'équivalence

$$(x+yi)^2 = a+bi \iff \begin{cases} x^2-y^2 = a\\ 2xy = b.\end{cases}$$

Si $(x+yi)^2 = a+bi$, il vient $x^2+y^2 = |x+yi|^2 = |(x+yi)^2| = |a+bi| = \sqrt{a^2+b^2}$. Nous avons donc *a fortiori* l'équivalence

$$(x+yi)^2 = a+bi \iff \begin{cases} x^2 - y^2 = a \\ 2xy = b \\ x^2 + y^2 = \sqrt{a^2+b^2} \end{cases}$$

et en faisant la somme et la différence de la première et de la troisième égalité, nous obtenons

$$(x+yi)^2 = a+bi \iff \begin{cases} 2x^2 = \sqrt{a^2+b^2} + a \\ 2y^2 = \sqrt{a^2+b^2} - a \\ 2xy = b. \end{cases}$$

Puisqu'on a $b^2 > 0$, les nombres réels $\sqrt{a^2+b^2}+a$ et $\sqrt{a^2+b^2}-a$ sont positifs, donc il vient $x = \frac{u}{\sqrt{2}}\sqrt{\sqrt{a^2+b^2}+a}$ et $y = \frac{v}{\sqrt{2}}\sqrt{\sqrt{a^2+b^2}-a}$ où $u = \pm 1$ et $v = \pm 1$. L'égalité $2xy = b$ implique que $xy$ a le signe de $b$, c'est-à-dire que l'on a $uv = \varepsilon$. En choisissant $u = 1$, il vient $v = \varepsilon$ ce qui donne la racine carrée $z = \frac{1}{\sqrt{2}}\left(\sqrt{\sqrt{a^2+b^2}+a} + i\varepsilon\sqrt{\sqrt{a^2+b^2}-a}\right)$. Si $z'$ est une autre racine carrée de $a+bi$, alors nous avons $z^2 = z'^2$ et $z \neq z'$, donc $z' = -z$. ∎

**Exemple.** Calculons les racines carrées du nombre complexe $3 - 4i$.
Pour tous nombres réels $x$ et $y$, on a les équivalences

$$(x+yi)^2 = 3-4i \iff \begin{cases} x^2 - y^2 = 3 \\ x^2 + y^2 = 5 \\ 2xy = -4 \end{cases} \iff \begin{cases} x^2 = 4 \\ y^2 = 1 \\ xy = -2 \end{cases}$$

$$\iff (x = 2, y = -1) \text{ ou } (x = -2, y = 1).$$

Les racines carrées de $3 - 4i$ sont donc $2 - i$ et $-2 + i$.

## 3. Argument d'un nombre complexe

Rappelons les propriétés des fonctions trigonométriques cosinus et sinus.

- Si $a$ et $b$ sont des nombres réels tels que $a^2 + b^2 = 1$, alors il existe un unique nombre réel $\theta \in [0, 2\pi[$ tel que $\cos\theta = a$ et $\sin\theta = b$.
- Pour tous nombres réels $x$ et $y$, on a l'équivalence

$$(\cos x = \cos y \text{ et } \sin x = \sin y) \iff \exists k \in \mathbb{Z},\ x - y = 2k\pi.$$

- Pour tous nombres réels $\theta$ et $\theta'$, on a les formules d'addition

$$\cos(\theta+\theta') = \cos\theta\cos\theta' - \sin\theta\sin\theta'$$
$$\sin(\theta+\theta') = \sin\theta\cos\theta' + \cos\theta\sin\theta'.$$



Si $z$ est un nombre complexe non nul, nous avons $(\mathcal{Re}\, z)^2 + (\mathcal{Im}\, z)^2 = |z|^2$ donc $\left(\frac{\mathcal{Re}\, z}{|z|}\right)^2 + \left(\frac{\mathcal{Im}\, z}{|z|}\right)^2 = 1$. Par suite, il existe un unique nombre réel $\theta \in [0, 2\pi[$ tel que $\mathcal{Re}\, z = |z|\cos\theta$ et $\mathcal{Im}\, z = |z|\sin\theta$, c'est-à-dire tel que $z = |z|\cos\theta + i|z|\sin\theta$.

**Définition**
Pour tout nombre complexe $z$ différent de 0, l'unique nombre réel $\theta \in [0, 2\pi[$ tel que $z = |z|(\cos\theta + i\sin\theta)$ s'appelle l'*argument* de $z$ et se note $\operatorname{Arg} z$.

Si $\varphi$ est un nombre réel tel que $z = |z|(\cos\varphi + i\sin\varphi)$, nous avons $\cos\varphi = \cos \operatorname{Arg} z$ et $\sin\varphi = \sin \operatorname{Arg} z$ et par conséquent $\varphi = \operatorname{Arg} z + 2k\pi$ où $k \in \mathbb{Z}$.
Si $z$ et $z'$ sont des nombres complexes non nuls, alors par définition de l'argument, on a l'équivalence : $z = z' \Leftrightarrow (|z| = |z'| \text{ et } \operatorname{Arg} z = \operatorname{Arg} z')$.

**Notation.** Soient $x$ et $y$ des nombres réels. S'il existe $k \in \mathbb{Z}$ tel que $x - y = 2k\pi$, on note cette propriété $x \equiv y\ [2\pi]$, ce qui se lit « $x$ est congru à $y$ modulo $2\pi$ ».

Avec cette notation, nous avons l'équivalence

$$(\cos x = \cos y \quad \text{et} \quad \sin x = \sin y) \iff x \equiv y\ [2\pi].$$

On en déduit que si $z$ est un nombre complexe non nul et s'écrit $z = |z|(\cos\varphi + i\sin\varphi)$, alors $\operatorname{Arg} z$ est l'unique nombre réel de l'intervalle $[0, 2\pi[$ tel que $\operatorname{Arg} z \equiv \varphi\ [2\pi]$.

**Proposition.** *Pour tous nombres complexes $z$ et $z'$ différents de 0, on a*

$$\operatorname{Arg}(zz') \equiv \operatorname{Arg} z + \operatorname{Arg} z'\ [2\pi] \quad \text{et} \quad \operatorname{Arg}(1/z) \equiv -\operatorname{Arg} z\ [2\pi].$$

**Démonstration.** Soient $z$ et $z'$ des nombres complexes non nuls. Posons $\theta = \operatorname{Arg} z$ et $\theta' = \operatorname{Arg} z'$ de sorte que l'on a $z = |z|(\cos\theta + i\sin\theta)$ et $z' = |z'|(\cos\theta' + i\sin\theta')$. Il vient

$$zz' = |z||z'|\left(\cos\theta\cos\theta' - \sin\theta\sin\theta' + i(\sin\theta\cos\theta' + \cos\theta\sin\theta')\right)$$
$$= |zz'|\left(\cos(\theta+\theta') + i\sin(\theta+\theta')\right)$$

d'où la première formule.
D'autre part, on a $1/z = \bar{z}/|z|^2$ et $\bar{z} = |z|(\cos\theta - i\sin\theta)$. On en déduit

$$\frac{1}{z} = \frac{1}{|z|}\left(\cos(-\theta) + i\sin(-\theta)\right)$$

d'où la seconde formule. ∎

**Formule de Moivre.** *Pour tout nombre réel $\theta$ et pour tout entier naturel $n$, on a*

$$(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta.$$

**Démonstration.** Soit $\theta$ un nombre réel. Démontrons la formule par récurrence. Cette formule est vraie lorsque $n = 0$ ou $n = 1$. Soit $n$ un entier supérieur ou égal à 2. Supposons la formule vraie pour l'entier $n-1$, c'est-à-dire supposons que l'on a $(\cos\theta + i\sin\theta)^{n-1} = \cos(n-1)\theta + i\sin(n-1)\theta$. Il vient

$$\begin{aligned}(\cos\theta + i\sin\theta)^n &= (\cos\theta + i\sin\theta)^{n-1}(\cos\theta + i\sin\theta)\\ &= \big(\cos(n-1)\theta + i\sin(n-1)\theta\big)(\cos\theta + i\sin\theta)\\ &= \big(\cos(n-1)\theta\,\cos\theta - \sin(n-1)\theta\,\sin\theta\big) + \\ &\qquad i\big(\cos(n-1)\theta\,\sin\theta + \sin(n-1)\theta\,\cos\theta\big)\\ &= \cos n\theta + i\sin n\theta \quad \text{d'après les formules de trigonométrie.}\end{aligned}$$

∎

**Corollaire.** *Pour tout nombre complexe $z$ différent de 0 et pour tout entier naturel $n$, on a $\operatorname{Arg}(z^n) \equiv n\operatorname{Arg} z\,[2\pi]$ et $|z^n| = |z|^n$.*

**Démonstration.** Soient $z$ un nombre complexe non nul et $n$ un entier naturel. Pour simplifier, posons $\theta = \operatorname{Arg} z$, de sorte que l'on a $z = |z|(\cos\theta + i\sin\theta)$. D'après la formule de Moivre, il vient $z^n = |z|^n(\cos\theta + i\sin\theta)^n = |z^n|(\cos n\theta + i\sin n\theta)$ donc $\operatorname{Arg}(z^n) \equiv n\theta\,[2\pi]$ et $|z^n| = |z|^n$. ∎

**Proposition.** *Soient $n$ un entier supérieur ou égal à 2 et $\alpha$ un nombre complexe différent de 0. Pour tout nombre complexe $z$, on a $z^n = \alpha$ si et seulement si $|z| = \sqrt[n]{|\alpha|}$ et $\operatorname{Arg} z = \dfrac{\operatorname{Arg}\alpha}{n} + \dfrac{2k\pi}{n}$, où $k$ est un entier naturel tel que $k \leqslant n-1$.*

**Démonstration.** Supposons $z^n = \alpha$. On a $|z|^n = |z^n| = |\alpha|$ d'où $|z| = \sqrt[n]{|\alpha|}$. De plus, on a $\operatorname{Arg}(z^n) = \operatorname{Arg}\alpha$ c'est-à-dire $n\operatorname{Arg} z \equiv \operatorname{Arg}\alpha\,[2\pi]$. Il existe donc $k \in \mathbb{Z}$ tel que $n\operatorname{Arg} z = \operatorname{Arg}\alpha + 2k\pi$ ou encore $\operatorname{Arg} z = \dfrac{\operatorname{Arg}\alpha}{n} + \dfrac{2k\pi}{n}$. Puisqu'on a par définition $0 \leqslant \operatorname{Arg} z < 2\pi$ et $0 \leqslant \operatorname{Arg}\alpha < 2\pi$, on en déduit $0 \leqslant n\operatorname{Arg} z < 2n\pi$ donc $-2\pi < n\operatorname{Arg} z - \operatorname{Arg}\alpha < 2n\pi$ ou encore $-2\pi < 2k\pi < 2n\pi$. En divisant par $2\pi$, nous obtenons $-1 < k < n$ c'est-à-dire $0 \leqslant k \leqslant n-1$ puisque $k$ est un nombre entier.

Réciproquement, supposons que $z$ est un nombre complexe non nul tel que $|z| = \sqrt[n]{|\alpha|}$ et $\operatorname{Arg} z = \dfrac{\operatorname{Arg}\alpha}{n} + \dfrac{2k\pi}{n}$ où $k$ est un entier. Alors $\cos(n\operatorname{Arg} z) = \cos\operatorname{Arg}\alpha$, $\sin(n\operatorname{Arg} z) = \sin\operatorname{Arg}\alpha$ et d'après la formule de Moivre, il vient

$$\begin{aligned} z^n &= |z|^n(\cos\operatorname{Arg} z + i\sin\operatorname{Arg} z)^n\\ &= |\alpha|\big(\cos(n\operatorname{Arg} z) + i\sin(n\operatorname{Arg} z)\big)\\ &= |\alpha|(\cos\operatorname{Arg}\alpha + i\sin\operatorname{Arg}\alpha) = \alpha.\end{aligned}$$

∎

**Exemple.** Les nombres complexes $z$ tels que $z^5 = 2$ sont les nombres complexes $\sqrt[5]{2}\left(\cos\dfrac{2k\pi}{5} + i\sin\dfrac{2k\pi}{5}\right)$, où $k = 0, 1, 2, 3$ ou 4.





**Définition**

Une racine $n$-ième de 1 s'appelle une racine $n$-ième de l'*unité*.

Les racines $n$-ièmes de l'unité sont les nombres complexes $\cos(2k\pi/n) + i\sin(2k\pi/n)$ où $k$ est un entier tel que $0 \leqslant k \leqslant n-1$. Toute racine $n$-ième de l'unité est donc une puissance du nombre $\cos(2\pi/n) + i\sin(2\pi/n)$, car d'après la formule de Moivre, on a l'égalité $\cos(2k\pi/n) + i\sin(2k\pi/n) = \big(\cos(2\pi/n) + i\sin(2\pi/n)\big)^k$ pour tout entier naturel $k$.

Toute racine $n$-ième de l'unité est de module 1.

Puisque deux nombres complexes non nuls sont égaux si et seulement s'ils ont même module et même argument, la proposition précédente affirme qu'un nombre complexe non nul a exactement $n$ racines $n$-ièmes.

**Exemples**

- Les racines carrées de l'unité sont 1 et $-1$, car pour tout nombre complexe $z$, on a les équivalences $z^2 - 1 = 0 \iff (z-1)(z+1) = 0 \iff (z = 1 \text{ ou } z = -1)$.
- Les racines cubiques de l'unité sont les nombres 1, $\cos(2\pi/3) + i\sin(2\pi/3) = -(1/2) + (\sqrt{3}/2)i$ et $\cos(4\pi/3) + i\sin(4\pi/3) = -(1/2) - (\sqrt{3}/2)i$.
  On pose traditionnellement $j = -(1/2) + (\sqrt{3}/2)i$, de sorte que les racines cubiques de l'unité sont 1, $j$ et $\bar{j}$. Remarquons que l'on a $j\,j^2 = 1 = |j|^2 = j\bar{j}$, donc $\bar{j} = j^2$. Enfin, puisqu'on a les égalités $0 = j^3 - 1 = (j-1)(j^2 + j + 1)$, on en déduit la relation $1 + j + j^2 = 0$.
- Soit $a = \sqrt{3}/2 + (1/2)i$. Puisque $\cos(\pi/6) = \sqrt{3}/2$ et $\sin(\pi/6) = 1/2$, les racines douzièmes de l'unité sont les nombres $1, a, a^2, \ldots, a^{11}$. Les racines quatrièmes de l'unité sont donc 1, $a^3 = i$, $a^6 = -1$, $a^9 = -i$ et l'on a $a^4 = j$, d'après la formule de Moivre.

**Remarque**

Nous avons montré au paragraphe 2 que l'on peut exprimer les racines carrées d'un nombre complexe par des formules algébriques. Il n'en va pas de même pour les racines $n$-ièmes lorsque $n \geqslant 3$ : dans ce cas, le calcul fait en général intervenir les fonctions cosinus et sinus.

## 4. Application à la trigonométrie

La formule de Moivre affirme que si $n \in \mathbb{N}$, alors pour tout nombre réel $\theta$, on a $\cos n\theta + i\sin n\theta = (\cos\theta + i\sin\theta)^n$. En développant $(\cos\theta + i\sin\theta)^n$ selon la formule du binôme de Newton, on exprime $\cos n\theta$ et $\sin n\theta$ au moyen des puissances de $\cos\theta$ et $\sin\theta$.

**Exemple.** On a $(\cos\theta + i\sin\theta)^3 = \cos 3\theta + i\sin 3\theta$. En développant selon la formule du binôme de Newton, on obtient

$$(\cos\theta + i\sin\theta)^3 = \cos^3\theta + 3i\cos^2\theta\sin\theta - 3\cos\theta\sin^2\theta - i\sin^3\theta$$

d'où

$$\begin{cases} \cos 3\theta = \cos^3\theta - 3\cos\theta\sin^2\theta \\ \sin 3\theta = 3\cos^2\theta\sin\theta - \sin^3\theta. \end{cases}$$

En utilisant l'identité $\cos^2\theta + \sin^2\theta = 1$, il vient

$$\begin{cases} \cos 3\theta = 4\cos^3\theta - 3\cos\theta \\ \sin 3\theta = 3\sin\theta - 4\sin^3\theta. \end{cases}$$

Réciproquement, on aimerait bien exprimer les puissances $\cos^n\theta$ et $\sin^n\theta$ au moyen de nombres $\cos k\theta$ et $\sin k\theta$. Cela est utile, par exemple en analyse pour calculer des primitives. Expliquons comment obtenir de telles formules.

**Lemme.** *Soit $\theta$ un nombre réel. Posons $z = \cos\theta + i\sin\theta$. Pour tout entier positif $n$, on a $2\cos n\theta = z^n + \dfrac{1}{z^n}$ et $2i\sin n\theta = z^n - \dfrac{1}{z^n}$.*

**Démonstration.** On a $|z|=1$, donc $z\neq 0$ et $|z^n|=1$. Il vient donc $1/z^n = \overline{z^n}/|z^n|^2 = \bar{z}^n$ et $z^n + 1/z^n = z^n + \bar{z}^n = 2\,\mathcal{R}e\, z^n$. D'après la formule de Moivre, on sait que $\cos n\theta = \mathcal{R}e\, z^n$ d'où l'égalité $2\cos n\theta = z^n + 1/z^n$. De même, on a $\sin n\theta = \mathcal{I}m\, z^n$ et $z^n - 1/z^n = z^n - \bar{z}^n = 2i\,\mathcal{I}m\, z^n$, d'où $2i\sin n\theta = z^n - 1/z^n$. ∎

**Exemple.** Soit $\theta$ un nombre réel. Posons $z = \cos\theta + i\sin\theta$. Nous avons

$$\begin{aligned} 2^4\cos^4\theta &= \left(z + \frac{1}{z}\right)^4 = z^4 + 4z^2 + 6 + 4\frac{1}{z^2} + \frac{1}{z^4} \\ &= z^4 + \frac{1}{z^4} + 4\left(z^2 + \frac{1}{z^2}\right) + 6 = 2\cos 4\theta + 8\cos 2\theta + 6 \end{aligned}$$

et l'on obtient la formule $\cos^4\theta = \dfrac{1}{8}\cos 4\theta + \dfrac{1}{2}\cos 2\theta + \dfrac{3}{8}$.

Nous avons également

$$\begin{aligned} 2^5 i^5 \sin^5\theta &= \left(z - \frac{1}{z}\right)^5 = z^5 - 5z^3 + 10z - 10\frac{1}{z} + 5\frac{1}{z^3} - \frac{1}{z^5} \\ &= z^5 - \frac{1}{z^5} - 5\left(z^3 - \frac{1}{z^3}\right) + 10\left(z - \frac{1}{z}\right) = 2i\sin 5\theta - 10i\sin 3\theta + 20i\sin\theta \end{aligned}$$

donc $\sin^5\theta = \dfrac{1}{16}\sin 5\theta - \dfrac{5}{16}\sin 3\theta + \dfrac{5}{8}\sin\theta$.





## Exercices

**1.** Calculer sous la forme $x + yi$, où $x$ et $y$ sont des nombres réels, les nombres complexes $z$ tels que

**a)** $z^4 + 4 = 0$ **b)** $z^3 + 1 = 0$ **c)** $z^3 + 2i = 0$.

**2.** Calculer sous la forme $x + yi$, où $x$ et $y$ sont des nombres réels, les racines carrées des nombres complexes :

**a)** $1 + i\sqrt{3}$ **b)** $5 + 12i$ **c)** $5 - 12i$ **d)** $\dfrac{1+i}{1-i}$.

**3.** Calculer les racines quatrièmes de $i$. En déduire $\cos(\pi/8)$ et $\sin(\pi/8)$.

**4.** Soit $z$ un nombre complexe non nul tel que $z^3 = i/\bar{z}$. Montrer que le module de $z$ est égal à 1. Calculer $z$.

**5.** Soit $z$ un nombre complexe non nul. Posons $a = z + (1/z)$.

**a)** Démontrer l'égalité $z^2(a^2 + a - 1) = z^4 + z^3 + z^2 + z + 1$.

**b)** Montrer que $a^2 + a - 1 = 0$ si et seulement si $z \neq 1$ et $z^5 = 1$.

**c)** En déduire que l'on a $\cos(2\pi/5) = (\sqrt{5} - 1)/4$.

**d)** Calculer $\cos(\pi/5)$ et $\cos(\pi/10)$.

**6.** Soit $z$ un nombre complexe de module 1 tel que $z \notin \mathbf{R}$ et soit $a$ un nombre complexe. Montrer que $|a - z| = |1 - az|$ si et seulement si $a$ est un nombre réel.

**7. a)** Déterminer les nombres complexes $z$ tels que $|z| = |1 + z|$.

**b)** Déterminer les nombres complexes $z$ tels que $|z| = |1 + z| = 1$.

**c)** Déterminer les nombres complexes $a, b, c$ tels que $|a| = |b| = |c| = 1$ et $a + b + c = 0$.

**8.** Soit $z$ un nombre complexe différent de 1.

**a)** Montrer que l'on a $\mathcal{R}e\,\dfrac{1+z}{1-z} = \dfrac{1-|z|^2}{|1-z|^2}$ et $\mathcal{I}m\,\dfrac{1+z}{1-z} = \dfrac{2\,\mathcal{I}m\, z}{|1-z|^2}$.

**b)** En déduire que $z$ est de module 1 si et seulement s'il existe un nombre réel $t$ tel que $z = \dfrac{ti+1}{ti-1}$.

**9.** Soient $a$ et $b$ des nombres réels tels que $a \neq b$. Montrer que pour tout nombre complexe $z$, on a l'équivalence $|z - a| = |z - b| \Leftrightarrow \mathcal{R}e\, z = (a+b)/2$.

**10.** Soient $u$ et $v$ des nombres complexes. Démontrer l'égalité

$$|u + v|^2 - |u - v|^2 = 4\,\mathcal{R}e(u\bar{v}).$$

**11.** Soit $a$ un nombre complexe. Considérons l'équation $(*)$ $\quad z - i\bar{z} = a$, où $z \in \mathbb{C}$. On pose $u = (1+i)/\sqrt{2}$.

**a)** Calculer $|u|$, $u^2$ et $(\bar{u})^2$.

**b)** On suppose $a = 0$. Trouver toutes les solutions de l'équation $(*)$.

**c)** Soit $z \in \mathbb{C}$. Montrer que l'on a $\mathcal{Im}\,(z^2) - |z|^2 \leqslant 0$.

**d)** On suppose que l'équation $(*)$ a au moins une solution. Montrer que $a^2$ est imaginaire et que l'on a $\mathcal{Im}\,(a^2) \leqslant 0$. En déduire que $a = |a|\bar{u}$.

**e)** On suppose que $a = |a|\bar{u}$.

**i)** Montrer que $a/2$ est solution de $(*)$

**ii)** Soient $z$ et $z'$ des nombres complexes tels que $z' = z + (a/2)$. Montrer que $z'$ est solution de $(*)$ si et seulement si $z - i\bar{z} = 0$.

**f)** Résoudre l'équation $(*)$.

**12.** Posons $E = \mathbb{C} \setminus \{-i\}$. Soit $f : E \to \mathbb{C}$ l'application définie par $f(z) = \dfrac{z-i}{z+i}$ quel que soit $z \in E$.

**a)** Montrer que l'application $f$ est injective.

**b)** Montrer que pour tout $z \in E$, on a $1 - f(z) \neq 0$.

**c)** Démontrer l'égalité $f(E) = \mathbb{C} \setminus \{1\}$.

**d)** Soit $z \in E$. Montrer que $1 - |f(z)|^2 = 4\dfrac{\mathcal{Im}\, z}{|z+i|^2}$.

**e)** Notons $\mathbb{U}$ l'ensemble des nombres complexes de module 1. Montrer que l'on a $f(\mathbb{R}) = \mathbb{U} \setminus \{1\}$.

**13.** Soit $a$ un nombre complexe tel que $|a| < 1$. Posons $D = \{\, z \in \mathbb{C} \mid |z| < 1 \,\}$ et $\mathbb{U} = \{\, z \in \mathbb{C} \mid |z| = 1 \,\}$.

**a)** Soit $z$ un nombre complexe tel que $|z| \leqslant 1$. Montrer que $1 - \bar{a}z \neq 0$ et que

$$1 - \frac{|z-a|^2}{|1-\bar{a}z|^2} = \frac{(1-|a|^2)(1-|z|^2)}{|1-\bar{a}z|^2}.$$

**b)** Montrer qu'un nombre complexe $z$ appartient à $D$ si et seulement si $\dfrac{z-a}{1-\bar{a}z}$ appartient à $D$.

**c)** Montrer qu'un nombre complexe $z$ appartient à $\mathbb{U}$ si et seulement si $\dfrac{z-a}{1-\bar{a}z}$ appartient à $\mathbb{U}$.

**d)** Soit $f : D \to D$ l'application définie par $f(z) = \dfrac{z-a}{1-\bar{a}z}$. Montrer que $f$ est une bijection.





**14.** Soient $x$ un nombre réel et $n$ un entier positif. Posons $z = \cos x + i \sin x$ et $a = \cos(x/2) + i\sin(x/2)$.

**a)** Soit $p$ un entier positif. Montrer que l'on a $z^p - 1 = 2ia^p \sin(px/2)$.

**b)** Supposons $z \neq 1$. Montrer que l'on a $1 + z + \cdots + z^n = a^n \dfrac{\sin((n+1)x/2)}{\sin(x/2)}$.

**c)** Calculer les sommes $1 + \cos x + \cdots + \cos(nx)$ et $\sin x + \sin(2x) + \ldots + \sin(nx)$.

**d)** Montrer que l'on a $C_n^0 + C_n^1 z + \cdots + C_n^n z^n = \left(2\cos(x/2)\right)^n a^n$.

**e)** Calculer la somme $C_n^0 + C_n^1 \cos x + \cdots + C_n^n \cos nx$.

**15.** Posons $z = \cos(2\pi/n) + i\sin(2\pi/n)$, où $n$ un entier supérieur ou égal à 2. Soient $a$ un nombre complexe non nul et $\alpha$ une racine $n$-ième de $a$.

**a)** Montrer que les racines $n$-ièmes de $a$ sont les nombres complexes $\alpha, z\alpha, \ldots, z^{n-1}\alpha$.

**b)** Montrer que la somme des racines $n$-ièmes de $a$ est égale à 0.

**c)** Soit $k$ un entier naturel. Montrer que $z^k = 1$ si et seulement si $k$ est multiple de $n$.

**d)** Posons $\omega = z^{n(n-1)/2}$. Calculer $\omega^2$. En déduire que l'on a $\omega = (-1)^{n-1}$.

**e)** Montrer que le produit des racines $n$-ièmes de $a$ est égal à $(-1)^{n-1}a$.

## Quelques réponses ou indications

1. **a)** On a $z^4 + 4 = (z^2 + 2i)(z^2 - 2i)$.

**b)** L'argument de $-1$ est égal à $\pi$, donc les solutions sont les nombres $\cos\frac{\pi}{3} + i\sin\frac{\pi}{3} = \sqrt{3}/2 + (1/2)i$, $\cos\left(\frac{\pi}{3} + \frac{2\pi}{3}\right) + i\sin\left(\frac{\pi}{3} + \frac{2\pi}{3}\right) = -1$ et $\cos\left(\frac{\pi}{3} + \frac{4\pi}{3}\right) + i\sin\left(\frac{\pi}{3} + \frac{4\pi}{3}\right) = \sqrt{3}/2 - (1/2)i$.

2. **a)** Les racines carrées de $1 + i\sqrt{3}$ sont $\pm((\sqrt{6}/2) + i(\sqrt{2}/2))$.

**b)** Les racines carrées de $5 + 12i$ sont $\pm(3 + 2i)$.

**c)** Les racines carrées de $5 - 12i$ sont les conjuguées des racines carrées de $5 + 12i$.

4. On a $|z|^3 = |z^3| = |i/\bar{z}| = 1/|z|$ donc $|z|^4 = 1$.

5. **c)** Montrer que les solutions de l'équation $x^2 + x - 1 = 0$ sont $2\cos(2\pi/5)$ et $2\cos(4\pi/5)$.

6. Calculer $(a - z)\overline{(a - z)}$ et $(1 - az)\overline{(1 - az)}$.

7. **b)** Utiliser **a)**.

**c)** Soit $a, b, c$ une solution. Puisque $a$ n'est pas nul, on peut poser $b' = b/a$ et $c' = c/a$. On a alors $-c' = 1 + b'$ et $|b'| = 1 = |-c'| = |1 + b'|$, de sorte qu'on peut appliquer **b)**. En posant $j = -(1/2) + (\sqrt{3}/2)i$, les solutions sont $(a, b, c) = (z, zj, zj^2)$ ou $(a, b, c) = (z, zj^2, zj)$, où $z$ est un nombre complexe quelconque de module 1.

11. b) Montrer que $z$ est solution si et seulement si $z^2$ est imaginaire et de partie imaginaire positive ou nulle. Montrer ensuite que cette condition est équivalente à $z^2 - (|z|u)^2 = 0$.
Les solutions sont les nombres $tu$, où $t \in \mathbb{R}$.

c) Pour tout nombre complexe $z$, on a $\mathcal{Im}\, z \leqslant |z|$.

f) Si $a \neq |a|\bar{u}$, alors d'après (d), l'équation $(*)$ n'a pas de solution. Si $a = |a|\bar{u}$, alors d'après la question précédente et (a), les solutions de $(*)$ sont les nombres $tu + (a/2)$, où $t \in \mathbb{R}$.

12. e) Utiliser (d).

13. a) Si $|z| \leqslant 1$, alors $|\bar{a}z| < 1$.

14. a) On a $z^p - 1 = a^p(a^p - \bar{a}^p)$.

c) Utiliser (b).

d) Développer $(1+z)^n$ selon la formule du binôme de Newton.

15. a) Les nombres complexes indiqués sont des racines $n$-ièmes de $a$ et ils sont deux à deux différents.

b) La somme $1 + z + \cdots + z^{n-1}$ est égale à 0.

c) Calculer l'argument de $z^k$.

d) On a $\omega^2 = 1$ d'après (c), donc $\omega = \pm 1$. De plus, on a l'égalité $\omega = 1$ si et seulement si l'entier $n(n-1)/2$ est multiple de $n$, c'est-à-dire si et seulement si $n$ est impair.

e) Utiliser (a) et (d).





# Chapitre 4

# Matrices

Ce chapitre est une introduction à l'algèbre linéaire. Nous y présentons le calcul matriciel, un outil qu'il est essentiel de maîtriser. Dans ce chapitre, la lettre $\mathbf{K}$ désigne $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.

## 1. Définitions et règles de calcul

**Définition**

Pour tous entiers positifs $n$ et $p$, une *matrice* $n \times p$ à *coefficients* dans $\mathbf{K}$ est un tableau d'éléments de $\mathbf{K}$ à $n$ lignes et à $p$ colonnes, que l'on note

$$\begin{bmatrix} a_{11} & \cdots & a_{1p} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{np} \end{bmatrix}$$

ou en abrégé $[a_{ij}]$. Les $a_{ij}$ s'appellent les *coefficients* de la matrice ; le premier indice est celui de la ligne et le second est celui de la colonne.

Soient $A=[a_{ij}]$ et $B=[b_{ij}]$ des matrices $n \times p$. On a $A=B$ si et seulement si $a_{ij}=b_{ij}$ pour tous $i \in \{1,\ldots,n\}$ et $j \in \{1,\ldots,p\}$. Ainsi, les matrices $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ et $\begin{bmatrix} 1 & 3 \\ 2 & 4 \end{bmatrix}$ ne sont pas égales.

**Notation.** L'ensemble des matrices $n \times p$ à coefficients dans $\mathbf{K}$ se note $M_{n,p}(\mathbf{K})$ et plus simplement $M_n(\mathbf{K})$ si $n = p$.

**Exemples**

- La matrice de $M_{2,3}(\mathbb{Q})$ définie par $a_{11} = 1$, $a_{12} = 2$, $a_{13} = 3$, $a_{21} = 4$, $a_{22} = -2$ et $a_{23} = 5$ est la matrice $\begin{bmatrix} 1 & 2 & 3 \\ 4 & -2 & 5 \end{bmatrix}$.
- La matrice de $M_{3,2}(\mathbb{Q})$ définie par $a_{ij} = i - j$ est la matrice $\begin{bmatrix} 0 & -1 \\ 1 & 0 \\ 2 & 1 \end{bmatrix}$.

- La matrice $n \times p$ dont tous les coefficients sont nuls se note par commodité $0$ et s'appelle la matrice nulle.

**Définitions**

Une matrice qui a le même nombre de colonnes et de lignes est dite *carrée*. Soit $A = [a_{ij}]$ une matrice carrée. Les nombres $a_{ii}$ s'appellent les coefficients *diagonaux* de $A$. On dit que la matrice $A$ est *diagonale* si l'on a $a_{ij} = 0$ dès que $i \neq j$, qu'elle est *triangulaire inférieure* si l'on a $a_{ij} = 0$ dès que $i < j$ et qu'elle est *triangulaire supérieure* si l'on a $a_{ij} = 0$ dès que $i > j$.

Pour ce qui est des matrices $2 \times 2$, les matrices diagonales sont celles de la forme $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$, les triangulaires inférieures sont les matrices $\begin{bmatrix} a & 0 \\ b & c \end{bmatrix}$ et les triangulaires supérieures sont les matrices $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$.

**Définitions**

Une matrice à une ligne s'appelle une *matrice-ligne* et une matrice à une colonne une *matrice-colonne*. Si $A = [a_{ij}]$ est une matrice $n \times p$, la $i$-ième ligne de la matrice $A$ est la matrice-ligne $[a_{i1} \cdots a_{ip}]$ et la $j$-ième colonne de la matrice $A$ est la matrice-colonne $\begin{bmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{bmatrix}$.

**Exemple.** La deuxième ligne de la matrice $\begin{bmatrix} 1 & 3 & -1 & 0 \\ 0 & 5 & 1 & 2 \\ -2 & 0 & 1 & 3 \end{bmatrix}$ est $[0\ 5\ 1\ 2]$ et sa troisième colonne est $\begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix}$.

## Opérations sur les matrices

Si $A = [a_{ij}]$ est une matrice de $M_{n,p}(\mathbf{K})$ et si $\lambda \in \mathbf{K}$, on note $\lambda A$ la matrice de $M_{n,p}(\mathbf{K})$ dont le coefficient à l'intersection de la ligne $i$ et de la colonne $j$ est $\lambda a_{ij}$. Par exemple, si $A = \begin{bmatrix} -1 & 0 & 2 \\ 1 & -2 & 1 \end{bmatrix}$, alors $3A = \begin{bmatrix} -3 & 0 & 6 \\ 3 & -6 & 3 \end{bmatrix}$.

De manière aussi simple, on définit la somme et la différence de deux matrices de même taille $n \times p$. Si $A = [a_{ij}]$ et $B = [b_{ij}]$ sont des matrices de $M_{n,p}(\mathbf{K})$, on note $A + B$ la matrice de $M_{n,p}(\mathbf{K})$ dont le coefficient à l'intersection de la ligne $i$ et de la colonne $j$ est $a_{ij} + b_{ij}$. De même, on définit $A - B = [a_{ij} - b_{ij}]$.

Par exemple, si $A = \begin{bmatrix} 2 & 0 & -1 & 1 \\ 1 & -1 & 0 & 1 \\ 0 & 0 & -2 & 3 \end{bmatrix}$ et $B = \begin{bmatrix} 7 & 6 & 5 & 4 \\ 0 & 0 & 1 & 0 \\ -1 & 2 & -3 & 4 \end{bmatrix}$, alors



$$A + B = \begin{bmatrix} 9 & 6 & 4 & 5 \\ 1 & -1 & 1 & 1 \\ -1 & 2 & -5 & 7 \end{bmatrix} \quad \text{et} \quad A - B = \begin{bmatrix} -5 & -6 & -6 & -3 \\ 1 & -1 & -1 & 1 \\ 1 & -2 & 1 & -1 \end{bmatrix}.$$

Autrement dit, multiplier une matrice par un élément de $\mathbf{K}$, ajouter et retrancher des matrices se fait coefficient par coefficient.

Nous allons maintenant définir le produit de deux matrices, en plusieurs étapes. Le calcul du produit de deux matrices est une opération plus compliquée que la somme ou la différence : pour effectuer ce calcul rapidement et sans faute, il faut de l'entraînement.

**Définition**

Soient $A = [a_1 \cdots a_p]$ une matrice de $M_{1,p}(\mathbf{K})$ et $B = \begin{bmatrix} b_1 \\ \vdots \\ b_p \end{bmatrix}$ une matrice de $M_{p,1}(\mathbf{K})$. Le *produit* de $A$ par $B$, noté $AB$, est la matrice $1 \times 1$ dont le coefficient est $a_1 b_1 + \cdots + a_p b_p$.

**Exemples**

- Si $A = [1\ 2\ 1]$ et $B = \begin{bmatrix} 3 \\ -1 \\ 2 \end{bmatrix}$, alors $1 \times 3 + 2 \times (-1) + 1 \times 2 = 3$, par suite $AB = [3]$.
- Plus généralement, si $A = [a\ b\ c]$ et si $B = \begin{bmatrix} x \\ y \\ z \end{bmatrix}$, alors $AB = [ax + by + cz]$.

**Définition**

Soient $A$ une matrice de $M_{n,p}(\mathbf{K})$ et $B$ une matrice de $M_{p,1}(\mathbf{K})$. Le *produit* de $A$ par $B$, noté $AB$, est la matrice $n \times 1$ dont la $i$-ième ligne est le produit de la $i$-ième ligne de $A$ par la matrice-colonne $B$.

**Exemples**

- Soient $A = \begin{bmatrix} 1 & -1 & 2 \\ -2 & 3 & 0 \\ 0 & 1 & 1 \\ -3 & 0 & 1 \end{bmatrix}$ et $B = \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix}$. Il vient $[1\ -1\ 2] \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix} = [4]$,

  $[-2\ 3\ 0] \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix} = [-5]$, $[0\ 1\ 1] \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix} = [0]$ et $[-3\ 0\ 1] \begin{bmatrix} 1 \\ -1 \\ 1 \end{bmatrix} = [-2]$.

  On a donc $AB = \begin{bmatrix} 4 \\ -5 \\ 0 \\ -2 \end{bmatrix}$.

- Si $a, b, c, d, x, y$ sont des nombres, on a $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} ax + by \\ cx + dy \end{bmatrix}$.

**Notation.** Soit $p$ un entier supérieur ou égal à 2. Pour tout entier $j \in \{1, 2, \ldots, p\}$, notons $E_j$ la matrice $p \times 1$ dont le coefficient de la $j$-ième ligne est égal à 1 et dont tous les autres coefficients sont nuls. Par exemple, si $p = 4$, il vient

$$E_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad E_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \quad E_3 = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \quad \text{et} \quad E_4 = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

Voici un lemme important et utile. La démonstration en est immédiate : il suffit d'appliquer la définition du produit matriciel.

**Lemme.** *Si $A$ est une matrice $n \times p$, alors le produit $AE_j$ est la $j$-ième colonne de la matrice $A$.*

Par exemple, si $A = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 3 \\ 2 & 1 & 0 & 1 \end{bmatrix}$, on a $AE_3 = \begin{bmatrix} 1 \\ 2 \\ 1 \\ 0 \end{bmatrix}$, qui est bien la troisième colonne de $A$.

Voici enfin la définition générale du produit de deux matrices.

**Définition**

Soient $A$ une matrice de $M_{n,p}(\mathbf{K})$ et $B$ une matrice de $M_{p,q}(\mathbf{K})$. Le *produit de $A$ par $B$*, noté $AB$, est la matrice $n \times q$ dont la $j$-ième colonne est le produit de $A$ par la $j$-ième colonne de $B$.

**Exemples**

- Calculons le produit de $\begin{bmatrix} 1 & 0 & 1 \\ 2 & 1 & 1 \\ 3 & 0 & -2 \\ 4 & -2 & 0 \end{bmatrix}$ par $\begin{bmatrix} 3 & 2 \\ -1 & 1 \\ 2 & 0 \end{bmatrix}$. On a

$$\begin{bmatrix} 1 & 0 & 1 \\ 2 & 1 & 1 \\ 3 & 0 & -2 \\ 4 & -2 & 0 \end{bmatrix} \begin{bmatrix} 3 \\ -1 \\ 2 \end{bmatrix} = \begin{bmatrix} 5 \\ 7 \\ 5 \\ 14 \end{bmatrix} \quad \text{et} \quad \begin{bmatrix} 1 & 0 & 1 \\ 2 & 1 & 1 \\ 3 & 0 & -2 \\ 4 & -2 & 0 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 2 \\ 5 \\ 6 \\ 6 \end{bmatrix},$$

d'où

$$\begin{bmatrix} 1 & 0 & 1 \\ 2 & 1 & 1 \\ 3 & 0 & -2 \\ 4 & -2 & 0 \end{bmatrix} \begin{bmatrix} 3 & 2 \\ -1 & 1 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 5 & 2 \\ 7 & 5 \\ 5 & 6 \\ 14 & 6 \end{bmatrix}.$$

- Si $a, b, c, d, x, y, z, t$ sont des nombres, il vient

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x & z \\ y & t \end{bmatrix} = \begin{bmatrix} ax + by & az + bt \\ cx + dy & cz + dt \end{bmatrix}.$$





- Soient $D$ et $D'$ des matrices diagonales $n \times n$. Si $D$ a pour coefficients diagonaux $d_1, \ldots, d_n$ et si $D'$ a pour coefficients diagonaux $d'_1, \ldots, d'_n$, alors
  la matrice $D + D'$ est diagonale, de coefficients diagonaux les $d_i + d'_i$,
  la matrice $DD'$ est diagonale, de coefficients diagonaux les $d_i d'_i$.

> Le produit de matrices $AB$ n'est défini que lorsque le nombre de colonnes de $A$ est égal au nombre de lignes de $B$.

Supposons que le produit de matrices $AB$ est bien défini et notons $L_i$ la $i$-ième ligne de $A$ et $C_j$ la $j$-ième colonne de $B$. Alors dans la matrice $AB$, le coefficient à l'intersection de la $i$-ième ligne et de la $j$-ième colonne est, d'après les définitions, le coefficient de la matrice $L_iC_j$ ; ce nombre est $a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{ip}b_{pj}$, si la matrice $A = [a_{ij}]$ possède $p$ colonnes et si $B = [b_{ij}]$.

**Définition**

Soit $k$ un entier supérieur ou égal à 2.
Une *combinaison linéaire* des matrices $A_1, A_2, \ldots, A_k$ de $M_{n,p}(\mathbf{K})$ est une matrice de $M_{n,p}(\mathbf{K})$ de la forme $\lambda_1 A_1 + \lambda_2 A_2 + \cdots + \lambda_k A_k$, où $\lambda_1, \lambda_2, \ldots, \lambda_k$ sont des éléments de $\mathbf{K}$.

**Exemples**

- Toute matrice de $M_2(\mathbf{R})$ est combinaison linéaire des quatre matrices suivantes :

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad \text{et} \quad \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

En effet, d'après les règles du calcul matriciel, on a pour tous nombres réels $x, y, z, t$

$$\begin{bmatrix} x & y \\ z & t \end{bmatrix} = x \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \frac{y+z}{2} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + \frac{z-y}{2} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} + t \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

- Si $n$ est un entier supérieur ou égal à 2, toute matrice de $M_{n,1}(\mathbf{K})$ est combinaison linéaire de $E_1, E_2, \ldots, E_n$. En effet, pour tous $x_1, x_2, \ldots, x_n \in \mathbf{K}$, on a

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = x_1 \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + x_2 \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix} + \cdots + x_n \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix} = x_1 E_1 + x_2 E_2 + \cdots + x_n E_n.$$

**Exercice.** Posons $A = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$. Trouver deux matrice $B$ et $C$ appartenant à $M_2(\mathbb{R})$ telles que l'ensemble des matrices $M \in M_2(\mathbb{R})$ vérifiant $MA = AM$ est l'ensemble des combinaisons linéaires de $B$ et $C$.

**Réponse.** Soient $x, y, z, t$ des nombres réels. Il vient

$$\begin{bmatrix} x & y \\ z & t \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} x & 2y \\ z & 2t \end{bmatrix} \quad \text{et} \quad \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}\begin{bmatrix} x & y \\ z & t \end{bmatrix} = \begin{bmatrix} x & y \\ 2z & 2t \end{bmatrix}.$$

On a donc $\begin{bmatrix} x & y \\ z & t \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}\begin{bmatrix} x & y \\ z & t \end{bmatrix}$ si et seulement si on a $z = 2z$ et $2y = y$ c'est-à-dire si et seulement si on a $y = z = 0$.

D'autre part, pour tous nombres réels $x$ et $t$ on a

$$\begin{bmatrix} x & 0 \\ 0 & t \end{bmatrix} = \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & t \end{bmatrix} = x\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + t\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

Les matrices $B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ et $C = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ répondent ainsi à la question.

Pour la matrice $A$ de l'exercice précédent, nous constatons qu'il existe des matrices $M$ telles que $AM \neq MA$. Étant données des matrices $A$ et $B$, même si les produits $AB$ et $BA$ sont définis, ils ne sont pas égaux en général.

**Notation.** On note $I_n$ la matrice $n \times n$ dont les coefficients diagonaux sont égaux à 1 et dont tous les autres coefficients sont nuls. Par exemple, nous avons

$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{et} \quad I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

### Règles de calcul

Si $A$ et $B$ sont des matrices appartenant à $M_{n,p}(\mathbf{K})$ et si $\lambda$ et $\mu$ sont des éléments de $\mathbf{K}$, on a

- $A + (B + C) = (A + B) + C$ et cette matrice est notée $A + B + C$
- $A + B = B + A$, $A + 0 = A$, $A - A = 0$
- $\lambda(A + B) = \lambda A + \lambda B$, $(\lambda + \mu)A = \lambda A + \mu A$
- $(\lambda\mu)A = \lambda(\mu A)$ et cette matrice est notée $\lambda\mu A$
- $I_n A = A$ et $AI_p = A$.

De plus, si $C$ et $D$ sont des matrices appartenant à $M_{p,q}(\mathbf{K})$, on a

- $\lambda(AC) = (\lambda A)C = A(\lambda C)$ et cette matrice est notée $\lambda AC$
- $(A + B)C = AC + BC$ et $A(C + D) = AC + AD$.

Toutes ces propriétés résultent de la définition des opérations sur les matrices et des règles de calcul suivantes dans $\mathbf{K}$ : $a + (b + c) = (a + b) + c$, $a + b = b + a$, $a + 0 = a$, $a - a = 0$, $ab = ba$, $a(bc) = (ab)c$ et $a(b + c) = ab + ac$.





On en déduit notamment que si $\lambda_1, \ldots, \lambda_r$ sont des éléments de $\mathbf{K}$, alors

$$A(\lambda_1 B_1 + \lambda_2 B_2 + \cdots + \lambda_r B_r) = \lambda_1 AB_1 + \lambda_2 AB_2 + \cdots + \lambda_r AB_r.$$

Voici la dernière règle de calcul pour le produit matriciel.

**Lemme.** *Soient $A \in M_{n,p}(\mathbf{K})$, $B \in M_{p,q}(\mathbf{K})$ et $C \in M_{q,r}(\mathbf{K})$. Alors on a $A(BC) = (AB)C$ et cette matrice est notée $ABC$.*

**Démonstration.** Pour tout entier $j \in \{1, \ldots, r\}$, notons $C_j$ la $j$-ième colonne de $C$. Par définition du produit matriciel, la $j$-ième colonne de $(AB)C$ est $(AB)C_j$ et la $j$-ième colonne de $A(BC)$ est le produit de $A$ par la $j$-ième colonne de $BC$. Or la $j$-ième colonne de $BC$ est $BC_j$, donc la $j$-ième colonne de $A(BC)$ est $A(BC_j)$.
Soit $X$ une matrice appartenant à $M_{q,1}(\mathbf{K})$. Démontrons que l'on a $(AB)X = A(BX)$. Si $q = 1$, alors il existe $x \in \mathbf{K}$ tel que $X = [x]$ et dans ce cas on a $(AB)X = xAB$ et $BX = xB$, par suite $(AB)X = A(BX)$. Si $q \geqslant 2$, alors il existe $x_1, x_2, \ldots, x_q \in \mathbf{K}$ tels que $X = x_1E_1 + \cdots + x_qE_q$. D'après les règles du calcul matriciel, on a $(AB)X = x_1(AB)E_1 + \cdots + x_q(AB)E_q$ et $A(BX) = x_1A(BE_1) + \cdots + x_qA(BE_q)$. Or on sait que $(AB)E_j$ est la $j$-ième colonne de $AB$ et de même que $BE_j$ est la $j$-ième colonne de $B$. Par définition du produit de $A$ par $B$, la $j$-ième colonne de $AB$ est le produit de $A$ par la $j$-ième colonne de $B$. On en déduit que l'on a $(AB)E_j = A(BE_j)$, pour tout $j \in \{1, \ldots, q\}$. Par suite on a $(AB)X = A(BX)$.
En particulier, il vient $(AB)C_j = A(BCj)$ pour tout $j \in \{1, \ldots, r\}$. Ainsi, les matrices $(AB)C$ et $A(BC)$ de $M_{n,r}(\mathbf{K})$ ont les mêmes colonnes, donc elles sont égales. ■

Une conséquence de ce lemme, c'est qu'on peut calculer un produit de matrices en choisissant successivement comme on veut les deux matrices consécutives dont il faut effectuer le produit.
Par exemple, il y a *a priori* cinq façons de calculer le produit de quatre matrices, correspondant aux parenthésages suivants :

$$((AB)C)D \;,\; (A(BC))D \;,\; A((BC)D) \;,\; A(B(CD)) \;,\; (AB)(CD).$$

Mais d'après le lemme, on a les égalités

$$A(BC)D = (A(BC))D = A((BC)D) = A(B(CD)) = (AB)(CD).$$

et ce produit de matrices se note simplement $ABCD$.

> Pour calculer un produit de matrices, inutile de mettre des parenthèses, mais il faut respecter l'ordre des facteurs.

**Notation.** Pour toute matrice $A \in M_n(\mathbf{K})$, on pose $A^0 = I_n$ et si $k$ est un entier positif, on note $A^k$ le produit de $A^{k-1}$ par $A$.

**Exemple.** Pour la matrice $A = \begin{bmatrix} 6 & 4 \\ -9 & -6 \end{bmatrix}$, on a $A^0 = I_2$, $A^1 = A$ et

$$A^2 = \begin{bmatrix} 6 & 4 \\ -9 & -6 \end{bmatrix} \begin{bmatrix} 6 & 4 \\ -9 & -6 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0.$$

On en déduit $A^k = 0$ pour tout entier $k \geqslant 2$.

**Définition**
Soit $A \in M_n(\mathbf{K})$. On dit que la matrice $A$ est *inversible* s'il existe une matrice $B \in M_n(\mathbf{K})$ telle que $AB = BA = I_n$.

**Lemme.** *Soit $A$ une matrice inversible de $M_n(\mathbf{K})$. Il existe une unique matrice $B$ appartenant à $M_n(\mathbf{K})$ telle que $AB = BA = I_n$. Cette matrice s'appelle l'inverse de $A$ et se note $A^{-1}$.*

**Démonstration.** Soient $B$ et $C$ des matrices de $M_n(\mathbf{K})$ telles que $AB = CA = I_n$. Il vient $C = CI_n = C(AB) = (CA)B = I_nB = B$. ∎

**Exemples**

- La matrice $A = \begin{bmatrix} 19 & 7 \\ 8 & 3 \end{bmatrix}$ est inversible et $A^{-1} = \begin{bmatrix} 3 & -7 \\ -8 & 19 \end{bmatrix}$.
- Pour toute matrice inversible $A \in M_n(\mathbf{K})$, la matrice $A^{-1}$ est inversible et l'on a $(A^{-1})^{-1} = A$.
- Une matrice diagonale est inversible si et seulement si ses coefficients diagonaux sont tous non nuls : précisément, si $D$ est la matrice diagonale de coefficients diagonaux $a_1, \dots, a_n$ et si aucun des $a_i$ n'est nul, alors $D^{-1}$ est la matrice diagonale de coefficients diagonaux $1/a_1, \dots, 1/a_n$. Cela résulte du calcul du produit de deux matrices diagonales.

La proposition suivante énonce deux règles de calcul importantes concernant les matrices inversibles : ces règles affirment que dans une égalité entre produits de matrices, on peut simplifier à droite ou à gauche par une matrice inversible.

**Proposition.** *Soient $B, C$ des matrices de $M_{n,p}(\mathbf{K})$.*
*i) Si $A$ est une matrice inversible de $M_n(\mathbf{K})$ et si $AB = AC$, alors $B = C$.*
*ii) Si $A$ est une matrice inversible de $M_p(\mathbf{K})$ et si $BA = CA$, alors $B = C$.*

**Démonstration.** Supposons que $A$ est une matrice inversible de $M_n(\mathbf{K})$ et que l'on a $AB = AC$. Multiplions à gauche par $A^{-1}$ les deux membres de cette égalité.





Il vient $A^{-1}AB = A^{-1}AC$. Puisque $A^{-1}A = I_n$, cette égalité s'écrit $I_nB = I_nC$. On a $I_nB = B$ et $I_nC = C$ d'après les règles de calcul, d'où $B = C$.
On démontre (ii) de la même manière. ∎

**Proposition.** *Soient $A$ et $B$ des matrices de $M_n(\mathbf{K})$. Si $A$ et $B$ sont inversibles, alors $AB$ est inversible et $(AB)^{-1} = B^{-1}A^{-1}$.*

**Démonstration.** Soient $A$ et $B$ des matrices inversibles de $M_n(\mathbf{K})$. On a

$$(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AI_nA^{-1} = AA^{-1} = I_n$$

et

$$(B^{-1}A^{-1})(AB) = B^{-1}(A^{-1}A)B = B^{-1}I_nB = B^{-1}B = I_n.$$ ∎

Plus généralement, si $A_1, A_2, \dots, A_r$ sont des matrices inversibles de $M_n(\mathbf{K})$, alors le produit $A_1A_2\cdots A_r$ est inversible et $(A_1A_2\cdots A_r)^{-1} = A_r^{-1}\cdots A_2^{-1}A_1^{-1}$. Un produit de matrices inversibles est donc inversible.
En particulier, on a le résultat suivant.

**Corollaire.** *Soit $A$ une matrice de $M_n(\mathbf{K})$. Si $A$ est inversible, alors pour tout entier positif $k$, la matrice $A^k$ est inversible et $(A^k)^{-1} = (A^{-1})^k$.*

Introduisons une dernière opération sur les matrices.

**Définition**
Soit $A = [a_{ij}]$ une matrice de $M_{n,p}(\mathbf{K})$. On appelle *transposée* de $A$ la matrice de $M_{p,n}(\mathbf{K})$ dont le coefficient à l'intersection de la ligne $i$ et de la colonne $j$ est $a_{ji}$. Cette matrice est notée ${}^tA$.

**Exemple.** Si $A = \begin{bmatrix} 1 & 0 \\ 2 & 1 \\ -1 & 3 \end{bmatrix}$, alors ${}^tA = \begin{bmatrix} 1 & 2 & -1 \\ 0 & 1 & 3 \end{bmatrix}$.

Remarquons que, d'une manière générale, la $i$-ième ligne de ${}^tA$ est la transposée de la $i$-ième colonne de $A$ et la $j$-ième colonne de ${}^tA$ est la transposée de la $j$-ième ligne de $A$.

**Propriétés de la transposée**

a) Si $A$ et $B$ sont des matrices de $M_{n,p}(\mathbf{K})$ et si $\lambda$ est un élément de $\mathbf{K}$, alors on a

$${}^t({}^tA) = A, \quad {}^t(\lambda A) = \lambda\,{}^tA \quad \text{et} \quad {}^t(A+B) = {}^tA + {}^tB.$$

b) De plus, si $C$ est une matrice de $M_{p,q}(\mathbf{K})$, on a ${}^t(AC) = {}^tC\,{}^tA$.

c) Si $A$ est une matrice carrée inversible, alors ${}^tA$ est inversible et $({}^tA)^{-1} = {}^t(A^{-1})$.
En effet, on a $({}^tA)({}^tA^{-1}) = {}^t(A^{-1}A)$ d'après (b) et ${}^t(A^{-1}A) = {}^tI_n = I_n$ ; de même on a ${}^t(A^{-1})({}^tA) = {}^t(AA^{-1}) = I_n$.

## 2. Matrices élémentaires

Soit $n$ un entier supérieur ou égal à 2.

- Pour tout entier $i \in \{1, 2, \dots, n\}$ et pour tout nombre $a \in \mathbf{K}$ tel que $a \neq 0$, on note $D_i(a)$ la matrice diagonale de $M_n(\mathbf{K})$ dont le $i$-ième coefficient diagonal est égal à $a$ et dont les autres coefficients diagonaux sont tous égaux à 1.
- Pour tous entiers $i, j \in \{1, 2, \dots, n\}$ tels que $i \neq j$ et pour tout nombre $\lambda \in \mathbf{K}$ on note $T_{ij}(\lambda)$ la matrice de $M_n(\mathbf{K})$ dont les coefficients diagonaux sont égaux à 1, dont le coefficient à l'intersection de la ligne $i$ et de la colonne $j$ est égal à $\lambda$ et dont tous les autres coefficients sont nuls.

### Exemples

- Si $n = 2$, il vient $D_1(a) = \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}$, $D_2(a) = \begin{bmatrix} 1 & 0 \\ 0 & a \end{bmatrix}$, $T_{12}(\lambda) = \begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix}$ et $T_{21}(\lambda) = \begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix}$.
- Si $n = 3$, on a par exemple $T_{32}(4) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 4 & 1 \end{bmatrix}$ et $T_{13}(2) = \begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$.

**Définition**

Soit $n$ un entier supérieur ou égal à 2. Une matrice de $M_n(\mathbf{K})$ de la forme $D_i(a)$ ou de la forme $T_{ij}(\lambda)$ s'appelle une matrice *élémentaire*.

Voici les premières propriétés des matrices élémentaires ; ces propriétés se déduisent aisément du calcul matriciel.

- On a ${}^t(D_i(a)) = D_i(a)$ et ${}^t(T_{ij}(\lambda)) = T_{ji}(\lambda)$.
- Les matrices $D_i(a)$ et $T_{ij}(\lambda)$ sont inversibles et l'on a $(D_i(a))^{-1} = D_i(1/a)$ et $(T_{ij}(\lambda))^{-1} = T_{ij}(-\lambda)$.
- Supposons qu'une matrice $P$ soit produit de matrices élémentaires. Puisqu'un produit de matrices inversibles est inversible, la matrice $P$ est inversible. De plus, $P^{-1}$ est un produit d'inverses de matrices élémentaires, donc $P^{-1}$ est produit de matrices élémentaires.





**Lemme.** *Soient $n$ un entier supérieur ou égal à 3 et $Q$ une matrice de $M_{n-1}(\mathbf{K})$. Soit $P$ la matrice de $M_n(\mathbf{K})$ dont la première colonne est égale à $E_1$ et dont les colonnes suivantes sont celles de $Q$ auxquelles on ajoute 0 en première ligne.*

- *Si $Q$ est une matrice élémentaire, alors $P$ est une matrice élémentaire.*
- *Si $Q$ est produit de matrices élémentaires, alors $P$ est produit de matrices élémentaires.*

Par exemple, soient $a, b \in \mathbb{R}$ tels que $a \neq 0$. On a le produit de matrices élémentaires $\begin{bmatrix} 1 & 0 \\ 0 & a \end{bmatrix} \begin{bmatrix} 1 & 0 \\ b & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ ab & a \end{bmatrix}$. Les matrices $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & a \end{bmatrix}$ et $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & b & 1 \end{bmatrix}$ sont des matrices élémentaires de $M_3(\mathbb{R})$. Puisqu'on a

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & a \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & b & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & ab & a \end{bmatrix},$$

cette dernière matrice est produit de matrices élémentaires.

Nous allons maintenant étudier le produit d'une matrice, à droite ou à gauche, par une matrice élémentaire.

### Opérations élémentaires sur les colonnes

Soient $p$ un entier supérieur ou égal à 2, $i$ et $j$ deux entiers différents compris entre 1 et $p$, $a$ un élément non nul de $\mathbf{K}$ et $\lambda$ un élément de $\mathbf{K}$. Soit $A$ une matrice de $M_{n,p}(\mathbf{K})$.

- Notons $A'$ la matrice obtenue à partir de $A$ en multipliant par $a$ la $j$-ième colonne, les autres colonnes restant inchangées.
- Notons $A''$ la matrice obtenue à partir de $A$ en ajoutant à la $j$-ième colonne le produit par $\lambda$ de la $i$-ième colonne, les autres colonnes restant inchangées.

On dit que les matrices $A'$ et $A''$ se déduisent de $A$ par *opération élémentaire sur les colonnes*.

Nous allons montrer que les matrices $A'$ et $A''$ s'obtiennent en multipliant $A$ à droite par certaines matrices élémentaires.

**Proposition.** *Avec les notations précédentes, on a $A' = AD_j(a)$ et $A'' = AT_{ij}(\lambda)$.*

**Démonstration.** Rappelons que l'on note $E_k$ la matrice de $M_{p,1}(\mathbf{K})$ dont le coefficient de la ligne $k$ est égal à 1 et dont tous les autres coefficients sont nuls. Rappelons également que si $M$ est une matrice à $p$ colonnes, alors par définition du produit matriciel, la $k$-ième colonne de $M$ est égale à $ME_k$.
Ainsi, la $k$-ième colonne de la matrice $AD_j(a)$ est égale à $AD_j(a)E_k$ et la $k$-ième colonne de la matrice $AT_{ij}(\lambda)$ est égale à $AT_{ij}(\lambda)E_k$. Si $k \neq j$, alors par définition des matrices élémentaires, on a $D_j(a)E_k = E_k$ et $T_{ij}(\lambda)E_k = E_k$. De plus, on a $D_j(a)E_j = aE_j$ et $T_{ij}(\lambda)E_j = E_j + \lambda E_i$, d'où le résultat. ■

**Exemples**

- Si $a, b, c, d, \lambda$ sont des nombres, on obtient

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix} T_{12}(\lambda) = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & c+\lambda a \\ b & d+\lambda b \end{bmatrix}$$

et

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix} T_{21}(\lambda) = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix} = \begin{bmatrix} a+\lambda c & c \\ b+\lambda d & d \end{bmatrix}.$$

- Si $a$ est un nombre, on a

$$\begin{bmatrix} 1 & 0 & 1 \\ -1 & 0 & 1 \\ 2 & 1 & 0 \end{bmatrix} T_{13}(a) = \begin{bmatrix} 1 & 0 & 1 \\ -1 & 0 & 1 \\ 2 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1+a \\ -1 & 0 & 1-a \\ 2 & 1 & 2a \end{bmatrix}$$

et si $a$ est non nul, il vient $\begin{bmatrix} 1 & 0 & 1 \\ -1 & 0 & 1 \\ 2 & 1 & 0 \end{bmatrix} D_1(a) = \begin{bmatrix} a & 0 & 1 \\ -a & 0 & 1 \\ 2a & 1 & 0 \end{bmatrix}$.

> Multiplier à droite par $D_j(a)$, c'est multiplier par $a$ la $j$-ième colonne.
> Multiplier à droite par $T_{ij}(\lambda)$, c'est ajouter $\lambda$ fois la $i$-ième colonne à la $j$-ième colonne.

**Exercice.** Posons $A = \begin{bmatrix} x & 3 & x' \\ y & 4 & y' \\ z & 5 & z' \end{bmatrix}$. Calculer la matrice $AT_{13}(1)T_{31}(-1)T_{13}(1)D_1(-1)$.

**Réponse.** Il vient successivement

$$AT_{13}(1) = \begin{bmatrix} x & 3 & x' \\ y & 4 & y' \\ z & 5 & z' \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} x & 3 & x+x' \\ y & 4 & y+y' \\ z & 5 & z+z' \end{bmatrix}$$

$$AT_{13}(1)T_{31}(-1) = \begin{bmatrix} x & 3 & x+x' \\ y & 3 & y+y' \\ z & 5 & z+z' \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} -x' & 3 & x+x' \\ -y' & 4 & y+y' \\ -z' & 5 & z+z' \end{bmatrix}$$

$$AT_{13}(1)T_{31}(-1)T_{13}(1) = \begin{bmatrix} -x' & 3 & x+x' \\ -y' & 4 & y+y' \\ -z' & 5 & z+z' \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} -x' & 3 & x \\ -y' & 4 & y \\ -z' & 5 & z \end{bmatrix}$$

$$AT_{13}(1)T_{31}(-1)T_{13}(1)D_1(-1) = \begin{bmatrix} -x' & 3 & x \\ -y' & 4 & y \\ -z' & 5 & z \end{bmatrix} \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} x' & 3 & x \\ y' & 4 & y \\ z' & 5 & z \end{bmatrix}.$$

Observons que dans l'exercice précédent la matrice calculée s'obtient à partir de la matrice $A$ en échangeant la première et la troisième colonne.





De manière générale, il est possible d'échanger deux colonnes d'une matrice en effectuant quatre opérations élémentaires successives. Précisément, si $p$ un entier supérieur ou égal à 2 et si $A$ est une matrice de $M_{n,p}(\mathbf{K})$, alors la matrice $AT_{ij}(1)T_{ji}(-1)T_{ij}(1)D_i(-1)$ se déduit de $A$ en échangeant les colonnes $i$ et $j$.

## Opérations élémentaires sur les lignes

Soient $n$ un entier supérieur ou égal à 2, $i$ et $j$ deux entiers différents compris entre 1 et $n$, $a$ un élément non nul de $\mathbf{K}$ et $\lambda$ un élément de $\mathbf{K}$. Soit $B$ une matrice de $M_{n,p}(\mathbf{K})$.

- Notons $B'$ la matrice obtenue à partir de $B$ en multipliant par $a$ la $i$-ième ligne de $B$, les autres lignes restant inchangées.
- Notons $B''$ la matrice obtenue à partir de $B$ en ajoutant à la $i$-ième ligne de $B$ le produit par $\lambda$ de la $j$-ième ligne, les autres lignes restant inchangées.

On dit que les matrices $B'$ et $B''$ se déduisent de $B$ par *opération élémentaire sur les lignes*.

Comme pour les opérations élémentaires sur les colonnes, on a la proposition suivante.

**Proposition.** *Avec les notations précédentes, on a* $B' = D_i(a)B$ *et* $B'' = T_{ij}(\lambda)B$.

**Démonstration.** D'après la règle de transposition d'un produit de matrices, on a ${}^t(D_i(a)B) = ({}^tB){}^t(D_i(a)) = ({}^tB)D_i(a)$ et ${}^t(T_{ij}(\lambda)B) = ({}^tB){}^t(T_{ij}(\lambda)) = ({}^tB)T_{ji}(\lambda)$. Puisque pour toute matrice $C$, la transposée de la $k$-ième ligne de $C$ est la $k$-ième colonne de la matrice ${}^tC$, on conclut grâce à la proposition page 59. ■

**Exemples**

- Si $a, b, c, d, \lambda$ sont des nombres, on a

$$T_{21}(\lambda) \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c+\lambda a & d+\lambda b \end{bmatrix}$$

et

$$T_{12}(\lambda) \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a+\lambda c & b+\lambda d \\ c & d \end{bmatrix}.$$

- Si $\lambda$ est un nombre, on obtient

$$T_{32}(\lambda) \begin{bmatrix} 1 & 0 & 1 \\ -1 & 0 & 1 \\ 2 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \lambda & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ -1 & 0 & 1 \\ 2 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ -1 & 0 & 1 \\ 2-\lambda & 1 & \lambda \end{bmatrix}.$$

> Multiplier à gauche par $D_i(a)$, c'est multiplier par $a$ la $i$-ième ligne.
> Multiplier à gauche par $T_{ij}(\lambda)$, c'est ajouter $\lambda$ fois la $j$-ième ligne à la $i$-ième ligne.

Comme pour les colonnes, on peut échanger deux lignes d'une matrice par une succession de quatre opérations élémentaires.

## 3. Utilisation des opérations élémentaires

Dans ce paragraphe, nous allons montrer qu'en effectuant des opérations élémentaires sur les lignes d'une matrice, on peut obtenir une matrice plus simple. Les démonstrations qui figurent dans ce paragraphe sont techniques et peuvent dans un premier temps être laissées de côté : il faut se concentrer sur les énoncés.

Rappelons que l'on note $E_1$ la matrice de $M_{n,1}(\mathbf{K})$ dont tous les coefficients sont nuls, sauf celui sur la première ligne qui est égal à 1.

**Proposition.** *Soient $n$ un entier supérieur ou égal à 2 et $A \in M_{n,1}(\mathbf{K})$. Si la matrice-colonne $A$ n'est pas nulle, alors il existe une matrice $P \in M_n(\mathbf{K})$ produit de matrices élémentaires, telle que $PA = E_1$.*

**Démonstration.** Notons $a_i$ le coefficient de la $i$-ième ligne de la matrice $A$.

Supposons $a_i = 0$ pour tout $i \geqslant 2$. Puisque $A$ n'est pas la matrice nulle, c'est que $a_1 \neq 0$. En multipliant la première ligne de $A$ par $1/a_1$, on obtient $E_1$, autrement dit $D_1(1/a_1)A = E_1$.

Supposons qu'il existe $i \geqslant 2$ tel que $a_i \neq 0$ et posons $\lambda = (1 - a_1)/a_i$. Puisqu'on a $\lambda a_i + a_1 = 1$, en multipliant par $\lambda$ la $i$-ième ligne de $A$ et en l'ajoutant à la première, on obtient $T_{1i}(\lambda)A = \begin{bmatrix} 1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix}$. Pour $j \geqslant 2$, ajoutons ensuite $-a_j$ fois la première ligne à la $j$-ième : on obtient 0 comme coefficient sur la $j$-ième ligne. On en déduit

$$T_{n1}(-a_n) \cdots T_{21}(-a_2) T_{1i}(\lambda) A = E_1. \qquad \blacksquare$$

**Définition**

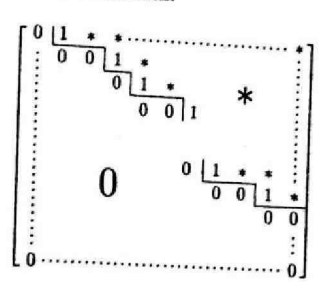
Soient $n$ un entier supérieur ou égal à 2 et $p$ un entier positif. Soit $A$ une matrice non nulle de $M_{n,p}(\mathbf{K})$. On dit que $A$ est *en échelons* lorsqu'elle possède les propriétés suivantes :

- chaque ligne est nulle ou bien son premier coefficient non nul est égal à 1,
- si une ligne est nulle, toutes les suivantes le sont,
- si la ligne $i$ a son premier coefficient non nul sur la colonne $j$, alors le premier coefficient non nul de la ligne $i+1$ est sur une colonne $k > j$.





Voici le schéma d'une matrice en échelons.



**Exemples**

- Il n'y a qu'une matrice $n \times 1$ en échelons, c'est la matrice $E_1$.
- Les matrices $2 \times 2$ en échelons sont les matrices de la forme
$$\begin{bmatrix} 1 & a \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \text{ et la matrice } \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}.$$
- Les matrices $2 \times 3$ en échelons sont les matrices de la forme
$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \end{bmatrix}, \begin{bmatrix} 1 & a & b \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & a & b \\ 0 & 0 & 0 \end{bmatrix},$$
$$\begin{bmatrix} 0 & 1 & a \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & a \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}.$$
- Les matrices $3 \times 3$ en échelons sont les matrices de la forme
$$\begin{bmatrix} 1 & a & b \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & a & b \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix},$$
$$\begin{bmatrix} 0 & 1 & a \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & a \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} \text{ et la matrice } \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

D'après les exemples ci-dessus, toutes les matrices $2 \times 2$ ou $3 \times 3$ en échelons sont triangulaires supérieures et dans le cas où la dernière ligne n'est pas nulle, les coefficients diagonaux sont égaux à 1. Le résultat est général.

**Proposition.** *Supposons que $A$ est une matrice carrée en échelons. Alors $A$ est triangulaire supérieure. De plus, si la dernière ligne n'est pas nulle, les coefficients diagonaux de $A$ sont tous égaux à 1.*

**Démonstration.** Par définition, une matrice en échelons est non nulle. La première ligne de $A$ n'est donc pas nulle, sinon toutes les lignes seraient nulles. Supposons que la dernière ligne non nulle de $A$ soit la $p$-ième, où $p$ est un entier positif tel que $p \leqslant n$. Alors aucune des $p$ premières lignes n'est nulle, car $A$ est en échelons. Pour tout entier $i$ compris entre 1 et $p$, notons $j_i$ l'indice de la colonne où apparaît le premier coefficient non nul de la $i$-ième ligne. La matrice $A$ étant en échelons, on a les inégalités strictes $j_p > j_{p-1} > \cdots > j_1$. Puisque $j_1 \geqslant 1$, on en déduit $j_k \geqslant k$ pour tout entier $k$ compris entre 1 et $p$. Les lignes d'indice strictement supérieur à $p$, s'il en existe, étant nulles, la matrice $A$ est triangulaire supérieure.

Supposons que la dernière ligne de $A$ est non nulle. On a donc $p = n$ et $n \geqslant j_n > j_{n-1} > \cdots > j_1 \geqslant 1$. Ces inégalités impliquent que l'on a $j_k = k$ pour tout entier $k$ compris entre 1 et $n$. Sur chaque ligne, le premier coefficient non nul est donc sur la diagonale de $A$. De plus, ces coefficients sont tous égaux à 1, car $A$ est en échelons. ■

**Notations**

- Si $A$ est une matrice $2 \times 3$, il est commode de noter $[0\ A]$ la matrice $2 \times 4$ dont la première colonne est nulle et dont les trois suivantes sont celles de $A$. Par exemple,

$$\text{si} \quad A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}, \quad \text{alors on a} \quad [0\ A] = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 0 & 4 & 5 & 6 \end{bmatrix}.$$

- De manière générale, si $A \in M_{n,p}(\mathbf{K})$, nous noterons $[0\ A]$ la matrice de $M_{n,p+1}(\mathbf{K})$ dont la première colonne est nulle et dont les $p$ dernières colonnes sont celles de $A$.
- Si $A \in M_{n,p}(\mathbf{K})$, on note $\begin{bmatrix} 1 & \bullet \\ 0 & A \end{bmatrix}$ une matrice de $M_{n+1,p+1}(\mathbf{K})$ de la forme suivante : les coefficients en bas à droite sont ceux de $A$ et la première colonne est $E_1 \in M_{n+1,1}(\mathbf{K})$.

Par exemple, si $A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}$, alors $\begin{bmatrix} 1 & \bullet \\ 0 & A \end{bmatrix} = \begin{bmatrix} 1 & a & b & c \\ 0 & 1 & 2 & 3 \\ 0 & 4 & 5 & 6 \end{bmatrix}$, où $a, b, c$ appartiennent à $\mathbf{K}$.

**Remarque**

Soit $A \in M_{n,p}(\mathbf{K})$ une matrice en échelons. La matrice $[0\ A]$ de $M_{n,p+1}(\mathbf{K})$ est alors en échelons. Toute matrice de $M_{n+1,p+1}(\mathbf{K})$ de la forme $\begin{bmatrix} 1 & \bullet \\ 0 & A \end{bmatrix}$ est également en échelons.

**Théorème.** *Soient $n$ un entier supérieur ou égal à 2 et $p$ un entier positif. Si $A$ est une matrice non nulle appartenant à $M_{n,p}(\mathbf{K})$, alors il existe une matrice $P \in M_n(\mathbf{K})$ produit de matrices élémentaires, telle que la matrice $PA$ est en échelons.*

**Démonstration.** Pour démontrer ce résultat, on va raisonner par récurrence sur le nombre de colonnes de $A$. Quel que soit l'entier positif $k$, notons $\mathscr{P}_k$ la propriété : pour tout entier $n \geqslant 2$ et pour toute matrice non nulle $A$ de $M_{n,k}(\mathbf{K})$, il existe une matrice $P \in M_n(\mathbf{K})$ produit de matrices élémentaires, telle que $PA$ est en échelons.





On sait déjà que $\mathscr{P}_1$ est vraie : c'est la première proposition de ce paragraphe.

Supposons $k \geqslant 2$ et la propriété $\mathscr{P}_{k-1}$ vraie. Soient un entier $n \geqslant 2$ et $A$ une matrice non nulle de $M_{n,k}(\mathbf{K})$. Notons $C$ la première colonne de $A$ et $B$ la matrice de $M_{n,k-1}(\mathbf{K})$ dont les colonnes sont les $k-1$ dernières de $A$ ; par commodité, nous noterons $A = [C\ B]$. Remarquons que pour toute matrice $P \in M_n(\mathbf{K})$, on a $PA = [PC\ PB]$.

Premier cas : $C = 0$. Dans ce cas la matrice $B$ est non nulle. Par hypothèse de récurrence, il existe une matrice $P \in M_n(\mathbf{K})$ produit de matrices élémentaires, telle que $PB$ est en échelons. Il vient $PA = [0\ PB]$ qui est en échelons d'après la remarque précédente.

Second cas : $C \neq 0$. D'après la première proposition du paragraphe, il existe une matrice $P_1 \in M_n(\mathbf{K})$ produit de matrices élémentaires telle que $P_1 C = E_1$. La matrice $P_1 A$ est alors de la forme $\begin{bmatrix} 1 & \bullet \\ 0 & A' \end{bmatrix}$, où $A' \in M_{n-1,k-1}(\mathbf{K})$. Si la matrice $A'$ est nulle, alors $P_1 A$ est en échelons. Plaçons-nous maintenant dans l'hypothèse $A' \neq 0$.

Supposons $n = 2$, c'est-à-dire supposons que la matrice $A'$ n'a qu'une ligne. Notons $a'$ le premier coefficient non nul de cette matrice-ligne. Si l'on multiplie par $1/a'$ la deuxième ligne de $P_1 A$, alors sur cette ligne le premier coefficient est nul et le premier coefficient non nul est égal à 1. La matrice $D_2(1/a')P_1 A$ est donc en échelons.

Si $n \geqslant 3$, par hypothèse de récurrence il existe une matrice $Q \in M_{n-1}(\mathbf{K})$, produit de matrices élémentaires, telle que $QA'$ est en échelons. Soit $P_2$ la matrice de $M_n(\mathbf{K})$ définie par $P_2 = \begin{bmatrix} 1 & 0 \\ 0 & Q \end{bmatrix}$. D'après le lemme page 59, la matrice $P_2$ est produit de matrices élémentaires, car $Q$ l'est. De plus, la matrice $P_2 P_1 A$ est de la forme $\begin{bmatrix} 1 & \bullet \\ 0 & QA' \end{bmatrix}$, donc est en échelons d'après la remarque précédente.

D'après le principe de récurrence, la propriété $\mathscr{P}_k$ est vraie quel que soit $k$. ■

**Exemple.** Pour illustrer le théorème précédent, considérons la matrice de $M_4(\mathbf{R})$

$$A = \begin{bmatrix} 1 & 2 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 2 \\ 1 & 1 & 1 & 1 \end{bmatrix}.$$

Retranchons la première ligne à la troisième et à la quatrième. Ces opérations élémentaires se traduisent matriciellement par l'égalité

$$T_{41}(-1)T_{31}(-1)A = \begin{bmatrix} 1 & 2 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & -2 & 0 & 2 \\ 0 & -1 & 0 & 1 \end{bmatrix}.$$

Ajoutons deux fois la deuxième ligne à la troisième et la deuxième ligne à la quatrième. On obtient l'égalité matricielle

$$T_{42}(1)T_{32}(2)T_{41}(-1)T_{31}(-1)A = \begin{bmatrix} 1 & 2 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 1 & 1 \end{bmatrix}.$$

Multiplions la troisième ligne par $1/2$, ce qui se traduit matriciellement par

$$D_3(1/2)T_{42}(1)T_{32}(2)T_{41}(-1)T_{31}(-1)A = \begin{bmatrix} 1 & 2 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}.$$

Enfin, retranchons la troisième ligne à la dernière. On obtient

$$T_{43}(-1)D_3(1/2)T_{42}(1)T_{32}(2)T_{41}(-1)T_{31}(-1)A = \begin{bmatrix} 1 & 2 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Cette dernière matrice est en échelons et elle se déduit bien de $A$ par opérations élémentaires sur les lignes.

**Proposition.** *Soit $T$ une matrice triangulaire supérieure de $M_n(\mathbf{K})$, où $n \geqslant 2$. Si les coefficients diagonaux de $T$ sont tous égaux à 1, alors $T$ est produit de matrices élémentaires.*

**Démonstration.** On démontre ce résultat par récurrence sur $n$. Si $n = 2$, on a $T = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$ qui est une matrice élémentaire.

Supposons $n \geqslant 3$ et la propriété démontrée pour $n-1$. Soient $T' \in M_{n-1}(\mathbf{K})$ et $L \in M_{1,n-1}(\mathbf{K})$ telles que $T = \begin{bmatrix} 1 & L \\ 0 & T' \end{bmatrix}$. Ainsi $T'$ est triangulaire supérieure et ses coefficients diagonaux sont tous égaux à 1. Par hypothèse de récurrence, $T'$ est produit de matrices élémentaires, donc inversible. Posons $Q' = (T')^{-1}$. Nous savons que la matrice $Q'$ est aussi produit de matrices élémentaires, ainsi que la matrice $Q = \begin{bmatrix} 1 & 0 \\ 0 & Q' \end{bmatrix}$. Il vient $QT = \begin{bmatrix} 1 & L \\ 0 & Q'T' \end{bmatrix} = \begin{bmatrix} 1 & L \\ 0 & I_{n-1} \end{bmatrix}$. Si l'on pose $L = [a_2 \cdots a_n]$, alors on a $T_{12}(-a_2) \cdots T_{1n}(-a_n)QT = I_n$, d'où

$$T = \Big(T_{12}(-a_2) \cdots T_{1n}(-a_n)Q\Big)^{-1} = Q^{-1}T_{1n}(a_n) \cdots T_{12}(a_2).$$

La matrice $T$ est donc produit de matrices élémentaires. ∎

Nous sommes maintenant en mesure de caractériser les matrices inversibles.



**Théorème.** *Si $A \in M_n(\mathbf{K})$ où $n \geqslant 2$, alors les propriétés suivantes sont équivalentes :*
*(i) la matrice $A$ est produit de matrices élémentaires*
*(ii) la matrice $A$ est inversible*
*(iii) il existe une matrice $B \in M_n(\mathbf{K})$ telle que $AB = I_n$*
*(iv) il existe une matrice $C \in M_n(\mathbf{K})$ telle que $CA = I_n$.*

**Démonstration.** Nous savons déjà que l'implication (i)⇒(ii) est vraie. Par définition d'une matrice inversible, on a (ii)⇒(iii) et (ii)⇒(iv).

Démontrons l'implication (iii)⇒(i). Supposons $AB = I_n$. Alors la matrice $A$ n'est pas nulle. Il existe donc une matrice $P \in M_n(\mathbf{K})$ produit de matrices élémentaires telle que la matrice $PA$ est en échelons. Puisque la matrice $P$ est inversible, il vient

$$(PA)(BP^{-1}) = P(AB)P^{-1} = PI_nP^{-1} = PP^{-1} = I_n.$$

Si la dernière ligne de $PA$ était nulle, alors tout produit de matrices $PAU$ aurait sa dernière ligne nulle, ce qui n'est pas le cas pour la matrice $U = BP^{-1}$. Par suite la matrice carrée $PA$ est en échelons et sa dernière ligne n'est pas nulle, donc $PA$ est triangulaire supérieure et ses coefficients diagonaux sont tous égaux à 1, d'après la proposition page 63. La proposition précédente affirme maintenant que $PA$ est produit de matrices élémentaires. Or on a $A = P^{-1}(PA)$ et la matrice $P^{-1}$ est produit de matrices élémentaires, donc la matrice $A$ aussi.

Ainsi les propriétés (i), (ii) et (iii) sont équivalentes et il nous reste seulement à démontrer que (iv) implique l'une d'entre elles.

Supposons $CA = I_n$. En utilisant l'implication (iii)⇒(ii), on en déduit que la matrice $C$ est inversible. Par suite $A = C^{-1}$, donc la matrice $A$ est inversible. ∎

**Remarque importante**

Supposons que $A$ et $B$ sont des matrices carrées $n \times n$. Nous venons de démontrer que si $AB = I_n$, alors les matrices $A$ et $B$ sont inversibles. Il s'ensuit $B = A^{-1}$ et $A = B^{-1}$. En particulier, si $AB = I_n$, alors $AB = BA = I_n$.

**Exercice.** Soit $A$ une matrice carrée $n \times n$.
a) Soit $k$ un entier positif. Calculer $(I_n - A)(I_n + A + A^2 + \cdots + A^k)$.
b) On suppose qu'il existe un entier positif $p$ tel que $A^p = 0$. Montrer que la matrice $I_n - A$ est inversible et calculer son inverse.

**Réponse**

a) On a $(I_n - A)(I_n + A) = (I_n - A)I_n + (I_n - A)A = I_n - A + A - A^2 = I_n - A^2$. Montrons, en raisonnant par récurrence, que l'on a $(I_n - A)(I_n + A + \cdots + A^k) = I_n - A^{k+1}$ pour tout entier positif $k$. Nous venons de vérifier que cette formule est vraie lorsque

$k = 1$. Supposons que $k$ est un entier positif pour lequel la formule est vraie. On a

$$\begin{aligned}(I_n - A)(I_n + A + \cdots + A^{k+1}) &= (I_n - A)(I_n + A + \cdots + A^k) + (I_n - A)A^{k+1} \quad \text{d'après les règles de calcul} \\ &= (I_n - A^{k+1}) + A^{k+1} - A^{k+2} \quad \text{par hypothèse de récurrence} \\ &= I_n - A^{k+2}.\end{aligned}$$

Cela montre que l'on a $(I_n - A)(I_n + A + \cdots + A^k) = I_n - A^{k+1}$ quel que soit l'entier positif $k$.

b) Puisque $A^p = 0$, on a $(I_n - A)(I_n + A + \cdots + A^{p-1}) = I_n - A^p = I_n$. D'après le théorème précédent, on en déduit que la matrice $I_n - A$ est inversible et que l'on a $(I_n - A)^{-1} = I_n + A + \cdots + A^{p-1}$.

## 4. Système d'équations linéaires

Dans ce paragraphe, $n$ est un entier positif et $p$ est un entier supérieur ou égal à 2. Un *système d'équations linéaires* à $n$ équations et $p$ inconnues est une équation de la forme $AX = B$, où $A \in M_{n,p}(\mathbf{K})$ et $B \in M_{n,1}(\mathbf{K})$ sont des matrices données et où l'on cherche la matrice-colonne $X \in M_{p,1}(\mathbf{K})$. La matrice $A$ s'appelle la matrice du système $AX = B$.

Si $A = [a_{ij}]$, $B = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$ et $X = \begin{bmatrix} x_1 \\ \vdots \\ x_p \end{bmatrix}$, le système $AX = B$ s'écrit également

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1p}x_p = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2p}x_p = b_2 \\ \vdots \qquad\qquad\qquad \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{np}x_p = b_n. \end{cases}$$

Résoudre le système $AX = B$, c'est trouver explicitement toutes les matrices $X \in M_{p,1}(\mathbf{K})$ telles que $AX = B$, s'il en existe.

**Proposition.** *Soient $A \in M_p(\mathbf{K})$ et $B \in M_{p,1}(\mathbf{K})$. Si la matrice $A$ est inversible, alors la seule solution du système $AX = B$ est la matrice $A^{-1}B$.*

**Démonstration.** D'après les règles du calcul matriciel, nous avons $A(A^{-1}B) = (AA^{-1})B = I_nB = B$. Réciproquement, soit $X$ une matrice de $M_{p,1}(\mathbf{K})$ telle que $AX = B$. Il vient $A^{-1}(AX) = A^{-1}B$, c'est-à-dire $(A^{-1}A)X = A^{-1}B$, ou encore $X = A^{-1}B$. ∎

**Exemple.** Soient $a$ et $b$ des nombres réels. Considérons le système

$$\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix}.$$



Puisque la matrice $\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$ est inversible, d'inverse $\begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix}$, le système ci-dessus a une et une seule solution, la matrice

$$\begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a - b \\ -a + 2b \end{bmatrix}.$$

**Proposition.** *Soient $A \in M_{n,p}(\mathbf{K})$ et $B \in M_{n,1}(\mathbf{K})$. Si la matrice $P \in M_n(\mathbf{K})$ est inversible, alors le système $AX = B$ a les mêmes solutions que le système $(PA)X = PB$.*

**Démonstration.** Soit $X \in M_{p,1}(\mathbf{K})$. Si $AX = B$, on multiplie cette égalité matricielle par $P$ et l'on en déduit $(PA)X = PB$. Réciproquement, si $(PA)X = PB$, on multiplie cette égalité matricielle par $P^{-1}$ ; il vient $P^{-1}(PA)X = P^{-1}(PB)$, c'est-à-dire $(P^{-1}P)AX = (P^{-1}P)B$, ou encore $AX = B$. ∎

Nous exploiterons cette proposition pour la résolution pratique des systèmes d'équations linéaires.

**Proposition.** *Soient $A \in M_{n,p}(\mathbf{K})$ et $B \in M_{n,1}(\mathbf{K})$. Supposons qu'il existe $X_0 \in M_{p,1}(\mathbf{K})$ telle que $AX_0 = B$. Les solutions du système $AX = B$ sont les matrices de la forme $X_0 + Y$, où $AY = 0$.*

**Démonstration.** Soit $X \in M_{p,1}(\mathbf{K})$. Posons $Y = X - X_0$. D'après les règles du calcul matriciel, on a $AX = A(X_0 + Y) = AX_0 + AY = B + AY$. On a donc $AX = B$ si et seulement si on a $AY = 0$. ∎

D'après la proposition précédente, si l'on connaît une solution particulière du système $AX = B$, alors pour avoir toutes les solutions il faut résoudre le système $AX = 0$. Avant d'exposer la méthode de résolution des systèmes d'équations linéaires, démontrons des conditions suffisantes pour que le système $AX = 0$ ait des solutions non nulles.

**Proposition.** *Soit $T \in M_p(\mathbf{K})$ une matrice triangulaire supérieure dont la dernière ligne est nulle. Alors le système $TX = 0$ a des solutions non nulles.*

**Démonstration.** On démontre ce résultat par récurrence sur $p$. Si $p = 2$, alors $T$ est de la forme $T = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$. Si $a = 0$, alors $T\begin{bmatrix} x \\ 0 \end{bmatrix} = 0$ pour tout $x \in \mathbf{K}$ et si $a \neq 0$, alors $T\begin{bmatrix} -bx/a \\ x \end{bmatrix} = 0$ pour tout $x \in \mathbf{K}$. La propriété est ainsi démontrée lorsque $p = 2$. Supposons $p \geqslant 3$ et la propriété vraie pour $p - 1$. Soient $a \in \mathbf{K}$, $L \in M_{1,p-1}(\mathbf{K})$ et $T' \in M_{p-1}(\mathbf{K})$ tels que $T = \begin{bmatrix} a & L \\ 0 & T' \end{bmatrix}$. Si $a = 0$, il vient $T(xE_1) = 0$ pour tout $x \in \mathbf{K}$. Supposons $a \neq 0$. La matrice $T'$ est triangulaire supérieure et sa dernière ligne est nulle, donc par hypothèse de récurrence, il existe des matrices $Y \in M_{p-1,1}(\mathbf{K})$

telles que $Y \neq 0$ et $T'Y = 0$. Pour une telle matrice $Y$, $LY$ est une matrice $1 \times 1$, donc $LY = [b]$, où $b \in \mathbf{K}$. Puisque $a \neq 0$, il existe $x \in \mathbf{K}$ tel que $ax + b = 0$. Soit $X \in M_{p,1}(\mathbf{K})$ la matrice-colonne dont le premier coefficient est $x$ et dont les suivants sont ceux de $Y$. Alors on a $X \neq 0$ et $TX = 0$. ∎

**Théorème.** *Soit $A \in M_p(\mathbf{K})$. La matrice $A$ est inversible si et seulement si la seule solution du système $AX = 0$ est $X = 0$.*

**Démonstration.** D'après une proposition précédente, on sait que si la matrice $A$ est inversible, alors la seule solution du système $AX = 0$ est $X = A^{-1}0 = 0$. Réciproquement, supposons que la seule solution du système $AX = 0$ est $X = 0$ et démontrons que la matrice $A$ est inversible. D'après l'hypothèse, la matrice $A$ est non nulle, donc il existe une matrice $P \in M_p(\mathbf{K})$ produit de matrices élémentaires telle que la matrice $PA$ est en échelons. Puisque la matrice $P$ est inversible, si $(PA)X = 0$, alors on a $AX = 0$ et donc $X = 0$ par hypothèse. D'après la proposition précédente, la matrice triangulaire supérieure $PA$ n'a pas sa dernière ligne nulle. Par suite la matrice en échelons $PA$ n'a que des 1 sur la diagonale. D'après la proposition page 66, la matrice $PA$ est produit de matrices élémentaires, donc est inversible. Puisqu'on a $A = P^{-1}(PA)$, on en déduit que la matrice $A$ est produit de matrices inversibles, donc est inversible. ∎

Le théorème ci-dessus affirme donc que si $A$ est une matrice carrée non inversible, alors le système $AX = 0$ a au moins une solution non nulle.

**Remarque**

Supposons que $A$ est une matrice carrée. Nous savons que si $A$ est inversible, alors le système $AX = B$ a une unique solution. Réciproquement, supposons que le système $AX = B$ a une unique solution notée $X_0$. Puisque toute solution est somme de $X_0$ et d'une solution de $AX = 0$, on en déduit que le système $AX = 0$ a une unique solution, par suite la matrice $A$ est inversible.

**Corollaire.** *Soit $A \in M_{n,p}(\mathbf{K})$. Si $n < p$, alors le système $AX = 0$ a au moins une solution non nulle.*

**Démonstration.** Soit $B \in M_p(\mathbf{K})$ la matrice carrée dont les $n$ premières lignes sont celles de $A$ et dont les lignes suivantes sont nulles. En particulier, la dernière ligne de la matrice $B$ est nulle. On en déduit que pour toute matrice $C \in M_p(\mathbf{K})$, la dernière ligne de $BC$ est nulle, par suite $BC \neq I_p$. La matrice $B$ n'est donc pas inversible. D'après le théorème précédent, il existe une matrice $X \in M_{p,1}(\mathbf{K})$ telle que $X \neq 0$ et $BX = 0$. Il s'ensuit $AX = 0$. ∎



Nous allons maintenant apprendre à résoudre un système d'équations linéaires.

Le premier cas à considérer est celui où $n = 1$, c'est-à-dire celui où il n'y a qu'une équation. Voici deux exemples de résolution d'une équation linéaire.

**Exemple 1.** Cherchons les matrices $\begin{bmatrix} x \\ y \end{bmatrix}$ de $M_{2,1}(\mathbf{R})$ telles que $-2x + y = 1$. Pour tous nombres réels $x$ et $y$, il vient

$$-2x + y = 1 \iff y = 1 + 2x$$

$$\iff \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x \\ 1+2x \end{bmatrix} \iff \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} + x \begin{bmatrix} 1 \\ 2 \end{bmatrix}.$$

Les matrices cherchées sont donc celles de la forme $\begin{bmatrix} 0 \\ 1 \end{bmatrix} + \lambda \begin{bmatrix} 1 \\ 2 \end{bmatrix}$, où $\lambda \in \mathbf{R}$.

**Exemple 2.** Soient $a \in \mathbf{R}$ et $A = [1\ 0\ -a\ 1]$. Cherchons les matrices $X = \begin{bmatrix} x \\ y \\ z \\ t \end{bmatrix}$ appartenant à $M_{4,1}(\mathbf{R})$ telles que $AX = 0$. Il vient

$$AX = 0 \iff x - az + t = 0$$

$$\iff \begin{bmatrix} x \\ y \\ z \\ t \end{bmatrix} = \begin{bmatrix} az - t \\ y \\ z \\ t \end{bmatrix} \iff \begin{bmatrix} x \\ y \\ z \\ t \end{bmatrix} = y \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} + z \begin{bmatrix} a \\ 0 \\ 1 \\ 0 \end{bmatrix} + t \begin{bmatrix} -1 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

De plus, si l'on a

$$y \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} + z \begin{bmatrix} a \\ 0 \\ 1 \\ 0 \end{bmatrix} + t \begin{bmatrix} -1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = y' \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} + z' \begin{bmatrix} a \\ 0 \\ 1 \\ 0 \end{bmatrix} + t' \begin{bmatrix} -1 \\ 0 \\ 0 \\ 1 \end{bmatrix},$$

il vient $\begin{bmatrix} az - t \\ y \\ z \\ t \end{bmatrix} = \begin{bmatrix} az' - t' \\ y' \\ z' \\ t' \end{bmatrix}$ et par suite $\begin{cases} y = y' \\ z = z' \\ t = t' \end{cases}$. Toute solution du système $AX = 0$ s'écrit donc de manière unique comme combinaison linéaire des matrices

$$\begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \quad \begin{bmatrix} a \\ 0 \\ 1 \\ 0 \end{bmatrix} \quad \text{et} \quad \begin{bmatrix} -1 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

### Méthode de Gauss

On suppose $n \geqslant 2$. Soit $A$ une matrice non nulle de $M_{n,p}(\mathbf{K})$. Nous savons qu'il existe une matrice $P \in M_n(\mathbf{K})$ produit de matrices élémentaires, telle que la matrice $PA$ est en échelons. Posons $P = P_r \cdots P_2 P_1$, où les matrices $P_i$ sont des matrices élémentaires. Chaque matrice $P_i$ est inversible. D'après une proposition page 69, il s'ensuit que les solutions du système $AX = B$ sont les solutions de chacun des systèmes suivants :

$$(P_1 A)X = P_1 B, \quad (P_2 P_1 A)X = P_2 P_1 B, \quad \cdots \quad (PA)X = PB.$$

Pratiquer la méthode de Gauss pour résoudre le système $AX = B$ consiste à effectuer sur les équations de ce système les opérations correspondant aux opérations élémentaires sur les lignes de la matrice $A$ pour se ramener au système $(PA)X = PB$, dont la matrice $PA$ est en échelons.

Voici, présentée sur des exemples, la méthode de résolution des systèmes d'équations linéaires.

**Exemple 3.** Pratiquons la méthode de Gauss pour trouver toutes les matrices

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} \in M_{3,1}(\mathbb{R}) \quad \text{telles que} \quad \begin{cases} x + 2y + z = 1 \\ 2x + 3y - z = 4 \\ 3x + y - z = 2. \end{cases}$$

Pour tous nombres réels $x, y, z$, il vient

$$\begin{cases} x + 2y + z = 1 \\ 2x + 3y - z = 4 \\ 3x + y - z = 2 \end{cases} \overset{(1)}{\iff} \begin{cases} x + 2y + z = 1 \\ -y - 3z = 2 \\ 3x + y - z = 2 \end{cases} \overset{(2)}{\iff} \begin{cases} x + 2y + z = 1 \\ y + 3z = -2 \\ -5y - 4z = -1 \end{cases}$$

$$\overset{(3)}{\iff} \begin{cases} x + 2y + z = 1 \\ y + 3z = -2 \\ 11z = -11 \end{cases} \iff \begin{cases} x + 2y + z = 1 \\ y + 3z = -2 \\ z = -1. \end{cases}$$

L'équivalence (1) s'obtient en retranchant deux fois la première équation à la deuxième. L'équivalence (2) s'obtient en retranchant trois fois la première équation à la troisième. Pour l'équivalence (3), on ajoute cinq fois la deuxième équation à la troisième. La matrice du dernier système est en échelons, la méthode de Gauss est donc terminée. On poursuit alors de la manière suivante :

$$\begin{cases} x + 2y + z = 1 \\ y + 3z = -2 \\ z = -1 \end{cases} \iff \begin{cases} x + 2y + z = 1 \\ y = 1 \\ z = -1 \end{cases} \iff \begin{cases} x = 0 \\ y = 1 \\ z = -1. \end{cases}$$

Il y a donc une et une seule solution au problème posé : la matrice $\begin{bmatrix} 0 \\ 1 \\ -1 \end{bmatrix}$.





**Exemple 4.** Soient $a, b$ et $m$ des nombres réels. Considérons le système d'équations linéaires

$$\begin{cases} x + y - z = a \\ y + mz = b \end{cases}$$

dont la matrice est en échelons. Pour tous nombres réels $x, y, z$, on a

$$\begin{cases} x + y - z = a \\ y + mz = b \end{cases} \iff \begin{cases} x = a - y + z \\ y = b - mz \end{cases} \iff \begin{cases} x = a - b + (m+1)z \\ y = b - mz \end{cases}$$

$$\iff \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} a - b + (m+1)z \\ b - mz \\ z \end{bmatrix}.$$

Les solutions sont donc définies par

$$\begin{cases} x = a - b + \lambda(m+1) \\ y = b - \lambda m \\ z = \lambda \end{cases} \quad \text{où } \lambda \in \mathbb{R}.$$

Le système d'équations considéré a une infinité de solutions. Une solution particulière est $X_0 = \begin{bmatrix} a - b \\ b \\ 0 \end{bmatrix}$ (correspondant à $\lambda = 0$). Les solutions du système $\begin{cases} x + y - z = 0 \\ y + mz = 0 \end{cases}$ sont les matrices $Y = \lambda \begin{bmatrix} m+1 \\ -m \\ 1 \end{bmatrix}$, où $\lambda \in \mathbb{R}$, et les solutions de notre sytème d'équations s'écrivent $X_0 + Y$.

**Exemple 5.** Soient $a$ et $b$ des nombres réels. Considérons le système d'équations linéaires

$$\begin{cases} x - 2y + t = a \\ x - y - z + 4t = b \\ x - 3y + z - 2t = 2a - b. \end{cases}$$

Pratiquons la méthode de Gauss pour nous ramener à un système dont la matrice est en échelons. Pour tous nombres réels $x, y, z, t$, nous avons

$$\begin{cases} x - 2y + t = a \\ x - y - z + 4t = b \\ x - 3y + z - 2t = 2a - b \end{cases} \iff \begin{cases} x - 2y + t = a \\ y - z + 3t = b - a \\ x - 3y + z - 2t = 2a - b \end{cases}$$

$$\iff \begin{cases} x - 2y + t = a \\ y - z + 3t = b - a \\ -y + z - 3t = a - b \end{cases} \iff \begin{cases} x - 2y + t = a \\ y - z + 3t = b - a. \end{cases}$$

Poursuivons de la manière suivante :

$$\begin{cases} x - 2y + t = a \\ y - z + 3t = b - a \end{cases} \iff \begin{cases} x = a + 2y - t \\ y = b - a + z - 3t \end{cases} \iff \begin{cases} x = -a + 2b + 2z - 7t \\ y = b - a + z - 3t \end{cases}$$

$$\iff \begin{bmatrix} x \\ y \\ z \\ t \end{bmatrix} = \begin{bmatrix} -a + 2b + 2z - 7t \\ b - a + z - 3t \\ z \\ t \end{bmatrix}$$

$$\iff \begin{bmatrix} x \\ y \\ z \\ t \end{bmatrix} = \begin{bmatrix} -a + 2b \\ b - a \\ 0 \\ 0 \end{bmatrix} + z \begin{bmatrix} 2 \\ 1 \\ 1 \\ 0 \end{bmatrix} + t \begin{bmatrix} -7 \\ -3 \\ 0 \\ 1 \end{bmatrix}.$$

**Exercice.** Soit la matrice $A = \begin{bmatrix} 1 & 1 & -1 \\ 3 & -1 & 1 \\ 1 & 3 & -3 \\ 1 & 1 & 1 \end{bmatrix}$ appartenant à $M_{4,3}(\mathbb{R})$.

a) Soient $a, b, c, d$ des nombres réels. Résoudre le système d'équations $AX = \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix}$.

b) En déduire une matrice $A' \in M_{3,4}(\mathbb{R})$ telle que $A'A = I_3$.

**Réponse**

a) Le système d'équations s'écrit

$$\begin{cases} x + y - z = a \\ 3x - y + z = b \\ x + 3y - 3z = c \\ x + y + z = d \end{cases} \iff \begin{cases} x + y - z = a \\ 4y - 4z = 3a - b \\ -2y + 2z = a - c \\ -2z = a - d \end{cases} \iff \begin{cases} x + y - z = a \\ 4y - 4z = 3a - b \\ 0 = 3a - b + 2(a - c) \\ 2z = -a + d \end{cases}$$

$$\iff \begin{cases} x = a - y + z \\ 4y = a - b + 2d \\ 2z = -a + d \\ 0 = 5a - b - 2c \end{cases} \iff \begin{cases} x = a/4 + b/4 \\ y = a/4 - b/4 + d/2 \\ z = -a/2 + d/2 \\ 5a - b - 2c = 0 \end{cases}$$

**Premier cas** : Si $5a - b - 2c \neq 0$, alors le système n'a pas de solution, car le dernier système d'égalités n'est satisfait par aucun nombres $x, y, z$.

**Second cas** : Supposons $5a - b - 2c = 0$. Alors le système a une unique solution qui est $x = a/4 + b/4$, $y = a/4 - b/4 + d/2$, $z = -a/2 + d/2$.

b) Posons $A' = \begin{bmatrix} 1/4 & 1/4 & 0 & 0 \\ 1/4 & -1/4 & 0 & 1/2 \\ -1/2 & 0 & 0 & 1/2 \end{bmatrix}$. Pour toute matrice $X \in M_{3,1}(\mathbb{R})$ et pour tous nombres réels $a, b, c, d$, on a donc d'après a)



$$AX = \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} \iff \begin{cases} X = A' \begin{bmatrix} a \\ b \\ d \\ d \end{bmatrix} \\ 5a - b - 2c = 0 \end{cases}$$

En particulier, il vient l'implication

$$AX = \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} \Longrightarrow X = A' \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix}.$$

On en déduit que pour toute matrice $X \in M_{3,1}(\mathbb{R})$, on a l'égalité $X = A'(AX)$, autrement dit $X = (A'A)X$. Choisissons pour $X$ la matrice $E_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$ ; puisque la matrice $(A'A)E_1$ est la première colonne de $A'A$, on en déduit que la première colonne de $A'A$ est $E_1$. De même, en choisissant pour $X$ les matrices $E_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$ et $E_3 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$, on en déduit que la deuxième colonne de $A'A$ est $E_2$ et que la troisième colonne de $A'A$ est $E_3$. On a donc $A'A = I_3$.

## Méthode de calcul de l'inverse d'une matrice

Soit $A \in M_p(\mathbf{K})$. Nous savons que la matrice $A$ est inversible si et seulement si, pour toute matrice $Y \in M_{p,1}(\mathbf{K})$, le système $AX = Y$ a une et une seule solution. De plus, si $A$ est inversible, alors $A^{-1}$ est la matrice du système $A^{-1}Y = X$. Pour déterminer si la matrice $A$ est inversible et pour calculer son inverse, on résout le système $AX = Y$, où $Y$ est une matrice dont tous les coefficients sont des lettres.

**Exemple.** Soit $m$ un nombre réel. Considérons la matrice

$$A = \begin{bmatrix} 1 & m & -2 \\ 1 & m+1 & m-2 \\ 2 & 2m+1 & 2m-4 \end{bmatrix}.$$

Soient $a, b, c$ des nombres réels. Pour tous nombres réels $x, y, z$, on a

$$A \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} a \\ b \\ c \end{bmatrix} \iff \begin{cases} x + my - 2z = a \\ x + (m+1)y + (m-2)z = b \\ 2x + (2m+1)y + (2m-4)z = c \end{cases}$$

$$\iff \begin{cases} x + my - 2z = a \\ y + mz = b - a \\ y + 2mz = c - 2a \end{cases}$$

$$\iff \begin{cases} x + my - 2z = a \\ \quad y + mz = b - a \\ \quad\quad mz = c - b - a. \end{cases}$$

Si $m = 0$, alors le système ci-dessus n'a pas de solution lorsque $c - b - a \neq 0$. Si $m = 0$, la matrice $A$ n'est donc pas inversible.

Supposons $m \neq 0$. Pour tous nombres réels $x, y, z$, il vient

$$A\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} a \\ b \\ c \end{bmatrix} \iff \begin{cases} mx = ma - m^2y + 2mz \\ y = 2b - c \\ mz = c - b - a \end{cases}$$

$$\iff \begin{cases} mx = (m-2)a - 2(m^2+1)b + (m^2+2)c \\ y = 2b - c \\ mz = c - b - a \end{cases}$$

$$\iff \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \frac{1}{m}\begin{bmatrix} m-2 & -2m^2-2 & m^2+2 \\ 0 & 2m & -m \\ -1 & -1 & 1 \end{bmatrix}\begin{bmatrix} a \\ b \\ c \end{bmatrix}.$$

La matrice $A$ est donc inversible et

$$A^{-1} = \frac{1}{m}\begin{bmatrix} m-2 & -2m^2-2 & m^2+2 \\ 0 & 2m & -m \\ -1 & -1 & 1 \end{bmatrix}.$$

Pour calculer l'inverse de la matrice carrée $A$, on résout le système $AX = Y$ où $Y$ est une matrice-colonne dont les coefficients sont des lettres.

## Exercices

**1.** Montrer que la matrice $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ est produit de trois matrices élémentaires.

**2.** Soient $a$, $b$ et $c$ des nombres complexes non nuls. Notons $A$, $B$ et $C$ les matrices suivantes de $M_3(\mathbf{C})$ :

$$A = T_{12}(a), \quad B = T_{23}(b) \quad \text{et} \quad C = T_{31}(c).$$

Montrer que $ABA^{-1}B^{-1}$ et $ACA^{-1}C^{-1}$ sont des matrices élémentaires.

**3.** Soient $A$ et $B$ des matrices de $M_n(\mathbf{K})$. Montrer que si la matrice $AB$ est inversible, alors les matrices $A$ et $B$ sont inversibles.



**4.** Pour tout nombre réel $\theta$, on pose $R(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$.

**a)** Montrer que l'on a $(R(\theta))^n = R(n\theta)$ pour tout $\theta \in \mathbb{R}$ et pour tout $n \in \mathbf{N}$.

**b)** Soient $a$ et $b$ des nombres réels. On suppose $b \neq 0$ et l'on considère la matrice

$$A = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}.$$

Montrer qu'il existe un unique nombre $\lambda > 0$ et un unique nombre $\theta \in ]0, 2\pi[$ tels que $A = \lambda R(\theta)$.

**c)** Calculer $\begin{bmatrix} -1 & -\sqrt{3} \\ \sqrt{3} & -1 \end{bmatrix}^n$ pour tout $n \in \mathbf{N}$.

**5.** Pour tout nombre réel $x$, on pose $A(x) = \begin{bmatrix} \operatorname{ch} x & \operatorname{sh} x \\ \operatorname{sh} x & \operatorname{ch} x \end{bmatrix}$.

**a)** Montrer que l'on a $A(x)A(y) = A(x+y)$ pour tous nombres réels $x$ et $y$.

**b)** Soit $x \in \mathbb{R}$. Montrer que la matrice $A(x)$ est inversible et calculer son inverse.

**6.** Montrer que la matrice suivante de $M_3(\mathbf{C})$ est inversible et calculer son inverse.

$$\begin{bmatrix} 2-i & i & 1 \\ i & 1 & 1+i \\ 3-i & i & 2 \end{bmatrix}$$

**7.** Pour tout nombre réel $t$, on pose

$$R(t) = \begin{bmatrix} e^t & 2te^t & (t^2-4t)e^t & 2+2(t-1)e^t \\ 0 & e^t & te^t & e^t - 1 \\ 0 & 0 & e^t & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

**a)** Montrer que l'on a $R(t)R(s) = R(t+s)$ pour tous nombres réels $t$ et $s$.

**b)** Soit $t \in \mathbb{R}$. Montrer que la matrice $R(t)$ est inversible et calculer son inverse.

**8.** Soient $J$, $K$ et $L$ les matrices de $M_2(\mathbf{C})$ définies par $J = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, $K = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$ et $L = JK$.

**a)** Montrer que l'on a $J^2 = K^2 = -I_2$ et $KJ = -JK$.

**b)** En déduire que l'on a $L^2 = -I_2$, $LJ = K$, $JL = -K$, $KL = J$ et $LK = -J$.

**c)** Soient $a, b, c, d$ des nombres réels. Calculer

$$(aI_2 + bJ + cK + dL)(aI_2 - bJ - cK - dL).$$

En déduire que si $a, b, c, d$ ne sont pas tous nuls, alors la matrice $aI_2 + bJ + cK + dL$ est inversible.

**9.** Soient $n$ un entier supérieur ou égal à 2 et $A$ une matrice appartenant à $M_n(\mathbf{K})$. On suppose les matrices $A$ et $I_n + A$ inversibles.

**a)** Montrer que la matrice $I_n + A^{-1}$ est inversible, d'inverse $A(I_n + A)^{-1}$.

**b)** Calculer $(I_n + A^{-1})^{-1} + (I_n + A)^{-1}$.

**10.** Soient $n$ un entier supérieur ou égal à 2 et $A, B$ des matrices de $M_n(\mathbf{K})$. On suppose la matrice $I_n + AB$ inversible et l'on note $S$ son inverse.

**a)** Montrer que l'on a $ABS = I_n - S$.

**b)** En déduire $(I_n + BA)BSA = BA$.

**c)** Montrer que la matrice $I_n + BA$ est inversible et calculer son inverse.

**11.** Soit $J$ la matrice de $M_2(\mathbb{R})$ définie par $J = \frac{1}{4}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$.

**a)** Calculer $J^2$ et $(I_4 - J)J$.

**b)** En déduire que les matrices $J$ et $I_4 - J$ ne sont pas inversibles.

**c)** Trouver toutes les matrices $X \in M_{4,1}(\mathbb{R})$ telles que $(I_4 - J)X = 0$.

**12. a)** Posons $D = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$. Démontrer que pour toute matrice $P \in M_3(\mathbb{R})$ inversible on a $(P^{-1}DP)^2 = -P^{-1}DP$ et $P^{-1}DP \neq -I_3$.

**b)** Soit $A \in M_3(\mathbb{R})$ telle que $A^2 = -A$ et $A \neq -I_3$. Calculer le produit $A(A + I_3)$. Montrer que la matrice $A$ n'est pas inversible.

**13.** Soient $n$ un entier supérieur ou égal à 2 et $A$ une matrice de $M_n(\mathbb{R})$ telle que $A^2 = A$. On suppose $A \neq 0$.

**a)** Montrer que la matrice $I_n - A$ n'est pas inversible.

**b)** Démontrer que pour tous nombres réels $r$ et $s$, la matrice $(I_n + rA)(I_n + sA)$ est combinaison linéaire de $I_n$ et $A$.

**c)** Soit $r$ un nombre réel différent de $-1$. Montrer que la matrice $I_n + rA$ est inversible et que son inverse est combinaison linéaire de $I_n$ et $A$.

**14.** Soient $n$ un entier supérieur ou égal à 2 et $A, B$ des matrices de $M_n(\mathbb{R})$ telles que $A^2 = A$ et $B^2 = B$.

**a)** On suppose que l'on a $AB = -BA$. Montrer que l'on a $AB = -ABA$, puis $AB = BA$. En déduire les égalités $AB = BA = 0$.

**b)** Démontrer l'équivalence suivante : $(A + B)^2 = A + B \Leftrightarrow AB = BA = 0$.

**c)** Trouver des matrices $2 \times 2$ non nulles $U$ et $V$, telles que $U^2 = U$, $V^2 = V$ et $UV = VU = 0$.





**15.** Soit $A$ la matrice de $M_2(\mathbb{R})$ définie par $A = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}$.

**a)** Montrer que la matrice $A$ est inversible et calculer $A^{-1}$.

**b)** Pour tout entier positif $n$, on pose $A^{-n} = (A^{-1})^n$. Démontrer que pour tout entier relatif $n$, on a $A^n = \begin{bmatrix} 2^n & n2^{n-1} \\ 0 & 2^n \end{bmatrix}$.

**c)** Soit $B \in M_2(\mathbb{R})$. Montrer que l'on a $AB = BA$ si et seulement s'il existe $a, b \in \mathbb{R}$ tels que $B = \begin{bmatrix} a & b \\ 0 & a \end{bmatrix}$.

**d)** Supposons qu'il existe $B \in M_2(\mathbb{R})$ telle que $B^2 = A$. Montrer que $AB = BA$.

**e)** Combien existe-il de matrices $B \in M_2(\mathbb{R})$ telles que $B^2 = A$ ?

**16.** Pour toute matrice $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ de $M_2(\mathbf{K})$, la *trace* de $A$ est le nombre $\operatorname{tr} A = a + d$.

**a)** Montrer que pour toutes matrices $A, B \in M_2(\mathbf{K})$ et pour tout $\lambda \in \mathbf{K}$, on a $\operatorname{tr}(\lambda A) = \lambda \operatorname{tr} A$, $\operatorname{tr}(A + B) = \operatorname{tr} A + \operatorname{tr} B$ et $\operatorname{tr}(AB) = \operatorname{tr}(BA)$.

**b)** En déduire que pour toutes matrices $A \in M_2(\mathbf{K})$ et $P \in M_2(\mathbf{K})$ où $P$ est inversible, on a $\operatorname{tr}(P^{-1}AP) = \operatorname{tr} A$.

**c)** Montrer qu'il n'existe pas de matrices $A, B \in M_2(\mathbf{K})$ telles que $AB - BA = I_2$.

**17.** Préciser pour quelles valeurs des nombres réels $a$ et $b$ le système d'équations linéaires

$$\begin{cases} x + ay + z = 3 \\ x + 2ay + z = 4 \\ x + y + bz = 3 \end{cases}$$

a zéro, une ou une infinité de solutions.

**18.** Soient $a, b, c$ et $m$ des nombres réels. On considère le système d'équations linéaires

$$\begin{cases} x - y + 2z = a \\ mx + (1 - m)y + 2(m - 1)z = b \\ 2x + my - (3m + 1)z = c. \end{cases} \qquad (*)$$

**a)** On suppose $m = -1$. Montrer qu'il existe des nombre réels $x, y, z$ vérifiant le système $(*)$ si et seulement si $c = 3a + b$.

**b)** On suppose $m = -1$ et $c = 3a + b$. Trouver une solution du système $(*)$ et montrer que ce système a une infinité de solutions.

**c)** On suppose $m \neq -1$. Montrer que le système $(*)$ a une unique solution. La calculer.

**d)** Pour quelles valeurs de $m$ la matrice

$$\begin{bmatrix} 1 & -1 & 2 \\ m & 1 - m & 2m - 2 \\ 2 & m & -3m - 1 \end{bmatrix}$$

est-elle inversible ? Dans ce cas, calculer son inverse.

19. Posons $A = \begin{bmatrix} 3 & 4 \\ 2 & 3 \\ -1 & -1 \end{bmatrix}$. Montrer qu'il n'existe aucune matrice $M \in M_{2,3}(\mathbb{C})$ telle que $AM = I_3$, mais qu'il en existe une infinité telles que $MA = I_2$.

20. Soit $A = [a_{ij}]$ une matrice de $M_n(\mathbf{K})$, triangulaire supérieure. On suppose que les coefficients diagonaux de $A$ sont tous non nuls.

**a)** Soit $B = [b_{ij}]$ la matrice de $M_n(\mathbf{K})$ définie en posant, pour tous indices $i, j$, $b_{ii} = 1$ et $b_{ij} = a_{ij}$ si $i \neq j$. Montrer que $B$ s'obtient en multipliant $A$ à gauche par des matrices élémentaires.

**b)** En déduire que la matrice $A$ est inversible.

21. Soit $A$ une matrice de $M_n(\mathbf{K})$. La somme des coefficients diagonaux de $A$ s'appelle la *trace* de $A$ et se note $\operatorname{tr} A$.

**a)** On suppose que $A$ est triangulaire supérieure. Calculer les coefficients diagonaux de $A^2$ au moyen des coefficients de $A$.

**b)** Posons $B = I_n - A$. Montrer que l'on a $A^2 = A$ si et seulement si $B^2 = B$.

**c)** Supposons que la matrice $A$ est triangulaire supérieure et que $A^2 = A$.

**(i)** Montrer que si $\operatorname{tr} A = n$, alors $A$ est inversible.

**(ii)** En déduire que si $\operatorname{tr} A = n$, alors $A = I_n$.

**(iii)** Montrer que si $\operatorname{tr} A = 0$, alors $A = 0$.

22. **a)** Soient $a_1, a_2, a_3, b_1, b_2, b_3$ des éléments de $K$. Calculer la matrice $\begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix} [b_1 \; b_2 \; b_3]$.

**b)** Soit $A$ une matrice-colonne à $n$ lignes et soit $B$ une matrice-ligne à $n$ colonnes, à coefficients dans $\mathbf{K}$. On suppose que $A$ n'est pas nulle. Montrer que les systèmes d'équations linéaires $ABX = 0$ et $BX = 0$, où $X \in M_{n,1}(\mathbf{K})$, ont les mêmes solutions.

**c)** Posons $M = AB$. Montrer qu'il existe un nombre $\lambda \in \mathbf{K}$ tel que $M^2 = \lambda M$.

23. Soit $n$ un entier au moins égal à 2.

**a)** Soient $(a_1, a_2, \ldots, a_n)$ et $(x_1, x_2, \ldots, x_n)$ des éléments de $\mathbb{R}^n$. Soit $p \in \{1, 2, \ldots, n\}$ tel que $|x_i| \leqslant |x_p|$ quel que soit $i \in \{1, 2, \ldots, n\}$. On suppose que l'on a $a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0$. Montrer que l'on a $|a_p||x_p| \leqslant s_p|x_p|$, où $s_p$ est la somme des nombres $|a_i|$ pour $i \neq p$.

**b)** Soit $A = [a_{ij}]$ une matrice de $M_n(\mathbb{R})$. On suppose que sur chaque ligne de $A$, la valeur absolue du terme diagonal est strictement supérieur à la somme des valeurs absolues des autres termes. Montrer que la matrice $A$ est inversible.





## Quelques réponses ou indications

1. Faire trois opérations élémentaires sur les lignes, de manière à obtenir $I_2$.

3. Si l'on pose $C = (AB)^{-1}$, alors l'inverse de $A$ est $BC$.

4. **b)** On a $\lambda = \sqrt{a^2 + b^2}$.

6. L'inverse est $\begin{bmatrix} 3-i & -i & i-2 \\ 4 & 1-i & -3 \\ i-4 & i & 3-i \end{bmatrix}$.

7. **b)** Calculer $R(0)$.

8. **c)** Utiliser **(a)** et **(b)**.

9. **b)** On a $(I_n + A^{-1})^{-1} + (I_n + A)^{-1} = I_n$.

10. **c)** Calculer $(I_n + BA)(I_n - BSA)$.

11. **a)** On a $J^2 = J$.

**b)** Raisonner par l'absurde.

12. **a)** On a $(P^{-1}DP)^2 = (P^{-1}DP)(P^{-1}DP) = P^{-1}D(PP^{-1})DP = P^{-1}DI_3DP = P^{-1}D^2P$.

**b)** Remarquer que, d'après la question a), il existe de telles matrices $A$.

13. **a)** Calculer $A(I_n - A)$.

**c)** L'inverse de $I_n + rA$ est $I_n - \frac{r}{r+1}A$.

14. **a)** Dans l'égalité $AB = -ABA$, remplacer dans le membre de droite $AB$ par $-BA$.

**c)** Par exemple, $U = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ et $V = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ conviennent.

15. **b)** Lorsque $n \in \mathbb{N}$, la formule se démontre par récurrence.

**e)** Utiliser **(d)** et **(c)** pour démontrer qu'il en existe deux.

16. **b)** D'après **(a)**, $\operatorname{tr}(P^{-1}AP) = \operatorname{tr}((AP)P^{-1})$.

**c)** On a $\operatorname{tr}(AB - BA) = 0$.

17. Il n'y a pas de solution lorsque $a = 0$ ou bien lorsque $a \neq 1$ et $b = 1$. Il y a une unique solution lorsque $a \neq 0$ et $b \neq 1$. Il y a une infinité de solutions lorsque $a = 1$ et $b = 1$.

18. **c)** L'unique solution est

$$\begin{cases} x = (1-m)a + b \\ y = \dfrac{(-3m^2 - 5m + 4)a + (3m+5)b - 2c}{m+1} \\ z = \dfrac{(-m^2 - 2m + 2)a + (m+2)b - c}{m+1}. \end{cases}$$

**d)** D'après **(a)**, **(b)** et **(c)**, la matrice est inversible si et seulement si $m \neq -1$. Utiliser **(c)** pour calculer l'inverse.

20. a) Multiplier $A$ par des matrices $D_i(a)$.

b) En appliquant une proposition du cours, montrer que la matrice $B$ définie dans (a) est inversible.

21. a) Les coefficients diagonaux de $A^2$ sont les carrés des coefficients diagonaux de $A$, car la matrice $A$ est triangulaire.

c) (i) Montrer que si $\operatorname{tr} A = n$, alors tous les coefficients diagonaux de $A$ sont égaux à 1.
(iii) Utiliser (b).

22. b) Puisque la matrice-colonne $A$ n'est pas nulle, l'un de ses coefficients n'est pas nul. Si le coefficient de la $i$-ième ligne n'est pas nul, considérer la $i$-ième équation des systèmes.

23. a) Le nombre $-a_p x_p$ est égal à la somme des $a_i x_i$ pour $i \neq p$.

b) Raisonner par l'absurde en faisant l'hypothèse que le système d'équations $AX = 0$ a une solution $X$ non nulle : appliquer le résultat de (a) en choisissant un indice $p$ convenable.





# Chapitre 5

# Déterminant d'une matrice

Nous avons vu, au chapitre précédent, l'importance théorique des matrices carrées inversibles : si $A$ est une matrice carrée, le système d'équations linéaires $AX = B$ a une unique solution si et seulement si la matrice $A$ est inversible. Nous allons maintenant introduire un outil de calcul pour déterminer si une matrice carrée est inversible. Dans ce chapitre, la lettre $\mathbf{K}$ désigne $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ et $n$ est un entier positif.

## 1. Définition

Si $A$ est une matrice appartenant à $M_n(\mathbf{K})$, le *déterminant* de $A$, noté $\det A$ ou bien $|a_{ij}|$ si $A$ est la matrice $[a_{ij}]$, est un élément de $\mathbf{K}$ que l'on définit par récurrence de la manière suivante :

- si $n = 1$ et $A = [a]$, alors $\det A = a$
- si $n \geqslant 2$ et $A = [a_{ij}]$, alors

$$\det A = a_{11}\Delta_{11} - a_{21}\Delta_{21} + \cdots + (-1)^{n+1}a_{n1}\Delta_{n1}$$

où $\Delta_{i1}$ est le déterminant de la matrice de $M_{n-1}(\mathbf{K})$ obtenue à partir de $A$ en rayant la première colonne et la $i$-ième ligne.

Si $n \geqslant 2$, le déterminant d'une matrice $n \times n$ est donc défini au moyen de $n$ déterminants de matrices $(n-1) \times (n-1)$. Par exemple, si $n = 2$ et $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, alors $\det A = a\Delta_{11} - c\Delta_{21} = ad - bc$, c'est-à-dire

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$$

Il est important de connaître parfaitement cette dernière formule.

**Exemples**

- Posons $A = \begin{bmatrix} 1 & 2 & 1 \\ -1 & 3 & 1 \\ 2 & 4 & 1 \end{bmatrix}$. En rayant la colonne 1 et la ligne 1 de la matrice $A$, on trouve la matrice $\begin{bmatrix} 3 & 1 \\ 4 & 1 \end{bmatrix}$, dont le déterminant est $\Delta_{11} = \begin{vmatrix} 3 & 1 \\ 4 & 1 \end{vmatrix} = -1$. De même, en rayant la colonne 1 et la ligne 2 de la matrice $A$, on trouve la matrice $\begin{bmatrix} 2 & 1 \\ 4 & 1 \end{bmatrix}$, dont le déterminant est $\Delta_{21} = \begin{vmatrix} 2 & 1 \\ 4 & 1 \end{vmatrix} = -2$. Enfin, en rayant la colonne 1 et la ligne 3, on obtient $\Delta_{31} = \begin{vmatrix} 2 & 1 \\ 3 & 1 \end{vmatrix} = -1$. Puisqu'on a

$$\det A = 1 \times \Delta_{11} - (-1) \times \Delta_{21} + 2 \times \Delta_{31},$$

on en déduit $\det A = -5$.

- Posons $B = \begin{bmatrix} 1 & 1 & 0 & -1 \\ 0 & 0 & 1 & 1 \\ 2 & 3 & 0 & 1 \\ -1 & 0 & 1 & 2 \end{bmatrix}$. Nous avons

$$\det B = \begin{vmatrix} 0 & 1 & 1 \\ 3 & 0 & 1 \\ 0 & 1 & 2 \end{vmatrix} + 2 \begin{vmatrix} 1 & 0 & -1 \\ 0 & 1 & 1 \\ 0 & 1 & 2 \end{vmatrix} + \begin{vmatrix} 1 & 0 & -1 \\ 0 & 1 & 1 \\ 3 & 0 & 1 \end{vmatrix} = -3 \begin{vmatrix} 1 & 1 \\ 1 & 2 \end{vmatrix} + 2 \begin{vmatrix} 1 & 1 \\ 1 & 2 \end{vmatrix} + \begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix} + 3 \begin{vmatrix} 0 & -1 \\ 1 & 1 \end{vmatrix}$$

et il s'ensuit $\det B = 3$.

Attention à ne pas confondre les notations : les crochets sont utilisés pour désigner une matrice, les barres verticales pour désigner le déterminant d'une matrice.

Calculer un déterminant en utilisant la définition est en général laborieux. Par exemple, le déterminant d'une matrice $4 \times 4$ est la somme de quatre déterminants de matrices $3 \times 3$, donc s'exprime à l'aide de douze déterminants de matrices $2 \times 2$, qu'il faut donc en principe calculer.

Nous allons maintenant établir des propriétés rendant plus simple le calcul d'un déterminant.

## 2. Propriétés du déterminant

**Proposition.** *Si $A$ est une matrice triangulaire, supérieure ou inférieure, alors le déterminant de $A$ est égal au produit des coefficients diagonaux de $A$.*

**Démonstration.** On démontre le résultat par récurrence sur le nombre $n$ de lignes de la matrice $A$. Le résultat est clair lorsque $n = 1$ ou $n = 2$. Supposons $n \geqslant 3$ et la propriété démontrée pour toute matrice triangulaire de $M_{n-1}(\mathbf{K})$. Considérons $A = [a_{ij}]$ une matrice triangulaire de $M_n(\mathbf{K})$.



*Premier cas* : $A$ est triangulaire supérieure. Puisqu'on a $a_{k1} = 0$ pour tout $k > 1$, il vient $\det A = a_{11}\Delta_{11}$. Or $\Delta_{11}$ est le déterminant d'une matrice triangulaire supérieure, donc par hypothèse de récurrence, on a $\Delta_{11} = a_{22} \cdots a_{nn}$. On en déduit $\det A = a_{11}a_{22} \cdots a_{nn}$.

*Second cas* : $A$ est triangulaire inférieure. Pour tout $i \geqslant 2$, $\Delta_{i1}$ est le déterminant d'une matrice triangulaire inférieure, dont la première ligne est nulle. Par exemple,

$$\text{si} \quad A = \begin{bmatrix} a & 0 & 0 & 0 \\ x & b & 0 & 0 \\ y & z & c & 0 \\ t & u & v & d \end{bmatrix} \quad \text{alors} \quad \Delta_{31} = \begin{vmatrix} 0 & 0 & 0 \\ b & 0 & 0 \\ u & v & d \end{vmatrix}.$$

Par hypothèse de récurrence, on a donc $\Delta_{i1} = 0$ pour tout $i \geqslant 2$, puisque le premier coefficient de la diagonale est nul. Comme dans le premier cas, il s'ensuit $\det A = a_{11}\Delta_{11} = a_{11}a_{22} \cdots a_{nn}$. ■

En particulier, on a $\det I_n = 1$.

Au chapitre précédent, nous avons défini les matrices élémentaires $D_i(a)$ et $T_{ij}(\lambda)$. Puisque ces matrices sont triangulaires, on a le corollaire suivant.

**Corollaire.** *Le déterminant de la matrice $D_i(a)$ est égal à $a$. Si $i \neq j$, le déterminant de la matrice $T_{ij}(\lambda)$ est égal à 1.*

Énonçons maintenant les propriétés qui expriment comment le déterminant d'une matrice dépend des lignes de cette matrice.

**Proposition.** *Soit $a \in \mathbf{K}$. Si l'on multiplie par $a$ l'une des lignes d'une matrice de $M_n(\mathbf{K})$, alors le déterminant est multiplié par $a$.*

**Démonstration.** On raisonne par récurrence, le résultat étant clair lorsque $n = 1$. Soit $A \in M_n(\mathbf{K})$, où $n \geqslant 2$. Notons $A'$ la matrice de $M_n(\mathbf{K})$ obtenue à partir de $A$ en multipliant la $i$-ième ligne par $a$, les autres lignes restant inchangées. Avec des notations évidentes, on a

$$\det A = a_{11}\Delta_{11} - a_{21}\Delta_{21} + \cdots + (-1)^{n+1}a_{n1}\Delta_{n1}$$
$$\det A' = a'_{11}\Delta'_{11} - a'_{21}\Delta'_{21} + \cdots + (-1)^{n+1}a'_{n1}\Delta'_{n1}.$$

Par hypothèse de récurrence, on a $\Delta'_{k1} = a\Delta_{k1}$ si $k \neq i$. De plus, on a $a'_{k1} = a_{k1}$ si $k \neq i$, $a'_{i1} = aa_{i1}$ et $\Delta'_{i1} = \Delta_{i1}$. On en déduit $\det A' = a \det A$. ■

En particulier, si une ligne de la matrice $A$ est nulle, il vient $\det A = 0 \times \det A = 0$. D'autre part, si $A \in M_n(\mathbf{K})$ et si $\lambda \in \mathbf{K}$, alors on a $\det(\lambda A) = \lambda^n A$, puisque chaque ligne est multiplié par $\lambda$.

En raisonnant par récurrence comme ci-dessus, on a aussi le résultat suivant.

**Proposition.** *Si les matrices $A$, $A'$ et $A''$ ne diffèrent que par leur $i$-ième ligne et si la $i$-ième ligne de $A$ est la somme des $i$-ièmes lignes de $A'$ et $A''$, alors on a $\det A = \det A' + \det A''$.*

**Proposition.** *Supposons $n$ supérieur ou égal à 2. Si l'on échange deux lignes d'une matrice de $M_n(\mathbf{K})$, alors le déterminant est multiplié par $-1$.*

**Démonstration.** Lorsque $n = 2$, le résultat est vrai puisqu'on a

$$\begin{vmatrix} c & d \\ a & b \end{vmatrix} = cb - da = -(ad - bc) = -\begin{vmatrix} a & b \\ c & d \end{vmatrix}.$$

Supposons $n \geqslant 3$ et procédons en trois étapes.

**1.** Montrons d'abord, en raisonnant par récurrence, que si l'on échange deux lignes consécutives, alors le déterminant est multiplié par $-1$. Supposons que dans la matrice $A \in M_n(\mathbf{K}$, on échange les lignes $i$ et $i+1$. Notons $A'$ la matrice ainsi obtenue et gardons les notations employées dans la démonstration précédente. Par hypothèse de récurrence, on a $\Delta'_{k1} = -\Delta_{k1}$ si $k \neq i, i+1$. De plus, on a $a'_{k1} = a_{k1}$ si $k \neq i, i+1$, $a'_{i1} = a_{(i+1)1}$, $a'_{(i+1)1} = a_{i1}$, $\Delta'_{i1} = \Delta_{(i+1)1}$ et $\Delta'_{(i+1)1} = \Delta_{i1}$. Il vient donc

$$\begin{cases} (-1)^{k+1}a'_{k1}\Delta'_{k1} = -(-1)^{k+1}a_{k1}\Delta_{k1} \quad \text{si} \quad k \neq i, j \\ (-1)^{i+1}a'_{i1}\Delta'_{i1} = -(-1)^{i+2}a_{(i+1)1}\Delta_{(i+1)1} \\ (-1)^{i+2}a'_{(i+1)1}\Delta'_{(i+1)1} = -(-1)^{i+1}a_{i1}\Delta_{i1}, \end{cases}$$

par suite on a $\det A' = -\det A$.

**2.** Montrons que si dans la matrice $A$, deux lignes sont égales, alors le déterminant de $A$ est nul. Supposons que les lignes $i$ et $j$ sont égales, où l'on a $i < j$, et raisonnons par récurrence sur $j - i$.

Supposons que l'on a $j - i = 1$, c'est-à-dire que les lignes $i$ et $j$ sont consécutives. Échangeons ces deux lignes. D'après l'étape 1, le déterminant de $A$ est multiplié par $-1$. Mais la matrice $A$ reste inchangée et par suite $\det A = 0$.

Supposons $j - i \geqslant 2$. Échangeons les lignes $j$ et $j-1$ et notons $B$ la matrice obtenue. D'après l'étape 1, on a $\det B = -\det A$. Dans la matrice $B$, les lignes $i$ et $j-1$ sont égales. Par hypothèse de récurrence, on a donc $\det B = 0$. On en déduit $\det A = 0$.

**3.** Démontrons maintenant la proposition. Notons $L_i$ et $L_j$ les lignes de $A$ considérées. Soit $M$ la matrice dont les lignes $i$ et $j$ sont toutes deux égales à $L_i + L_j$ et dont les autres lignes sont celles de $A$. Considérons la matrice $B$ dont les lignes $i$ et $j$ sont égales à $L_i$ et dont les autres lignes sont celles de $A$, et la matrice $C$ dont les lignes $i$ et $j$ sont égales à $L_j$ et dont les autres lignes sont celles de $A$.



En appliquant deux fois la proposition précédente, il vient

$$\det M = \det A + \det B + \det C + \det A',$$

où $A'$ est la matrice obtenue en échangeant les lignes $i$ et $j$. Puisque la matrice $M$ a deux lignes égales, on a $\det M = 0$, d'après l'étape 2. Pour la même raison, nous avons $\det B = \det C = 0$. On en déduit $\det A + \det A' = 0$, c'est-à-dire $\det A' = -\det A$. ∎

Énonçons le résultat obtenu dans l'étape 2 de la démonstration précédente.

**Corollaire.** *Supposons $n$ supérieur ou égal à 2. Si deux lignes de la matrice $A$ de $M_n(\mathbf{K})$ sont égales, alors le déterminant de la matrice $A$ est égal à 0.*

**Proposition.** *Supposons $n$ supérieur ou égal à 2. Si $A$ est une matrice de $M_n(\mathbf{K})$ et si $\lambda$ est un élément de $\mathbf{K}$, alors le déterminant de $A$ ne change pas si l'on ajoute à une ligne de $A$ le produit par $\lambda$ d'une autre ligne de $A$.*

**Démonstration.** Notons $L_1, L_2, \ldots, L_n$ les lignes de la matrice $A$. Soient $i$ et $j$ deux entiers différents compris entre 1 et $n$. Soit $A'$ la matrice de $M_n(\mathbf{K})$ dont toutes les lignes sont celles de $A$, sauf la $i$-ième qui est égale à $L_i + \lambda L_j$. Soit $B$ la matrice de $M_n(\mathbf{K})$ dont toutes les lignes sont celles de $A$, sauf la $i$-ième qui est égale à $L_j$. D'après les deux propositions précédentes, nous avons $\det A' = \det A + \lambda \det B$. Mais la matrice $B$ a ses $i$-ième et $j$-ième lignes égales, par suite $\det B = 0$. On en déduit $\det A' = \det A$. ∎

**Théorème.** *Si $A$ et $B$ sont des matrices de $M_n(\mathbf{K})$, alors $\det(AB) = (\det A)(\det B)$.*

**Démonstration.** C'est clair si $n = 1$. Supposons $n \geqslant 2$.

*Premier cas* : $A$ est une matrice élémentaire. Dans le chapitre précédent, nous avons montré que la matrice $D_i(a)B$ est obtenue à partir de $B$ en multipliant la $i$-ième ligne par $a$, et que la matrice $T_{ij}(\lambda)B$ est obtenue à partir de $B$ en ajoutant $\lambda$ fois la $j$-ième ligne à la $i$-ième. D'après les résultats que nous venons de voir, on a donc $\det(D_i(a)B) = a \det B$ et $\det(T_{ij}(\lambda)B) = \det B$. D'autre part, nous avons démontré que l'on a $\det D_i(a) = a$ et $\det T_{ij}(\lambda) = 1$. Il s'ensuit $\det(AB) = (\det A)(\det B)$.

*Deuxième cas* : $A$ est une matrice inversible. Dans ce cas, il existe un entier positif $r$ et des matrices élémentaires $P_1, \ldots, P_r$ telles que $A = P_1 \cdots P_r$ (voir le théorème page 67). On raisonne alors par récurrence sur $r$. Si $r = 1$, c'est le premier cas. Si $r \geqslant 2$, on a

$$\begin{aligned} \det(AB) &= \det(P_1(P_2 \cdots P_r B)) \\ &= (\det P_1)(\det(P_2 \cdots P_r B)) \quad \text{d'après le premier cas} \\ &= (\det P_1)(\det(P_2 \cdots P_r))(\det B) \quad \text{par hypothèse de récurrence} \\ &= (\det A)(\det B) \quad \text{d'après le premier cas.} \end{aligned}$$

*Troisième cas* : $A$ n'est pas inversible. Si $A=0$, alors $AB=0$ et $\det(AB)=\det A=0$ ; dans ce cas on a bien $\det(AB)=(\det A)(\det B)$. Supposons $A$ non nulle. D'après le théorème page 64, il existe $P\in M_n(\mathbf{K})$ produit de matrices élémentaires, telle que la matrice $PA$ est en échelons. Puisque la matrice $A$ n'est pas inversible et que la matrice $P$ l'est, la matrice $PA$ n'est pas inversible. En particulier, la dernière ligne de la matrice $PA$ est nulle et donc celle de la matrice $PAB$ également. Il s'ensuit $\det(PA)=\det(PAB)=0$. D'autre part, la matrice $P$ est inversible, par suite $\det(PA)=(\det P)(\det A)$ et $\det(PAB)=(\det P)(\det(AB))$ d'après le deuxième cas. Enfin, on a $P=P_1\cdots P_r$ où $P_i$ est une matrice élémentaire. D'après le premier cas et en raisonnant par récurrence sur $r$, il vient $\det P=(\det P_1)\cdots(\det P_r)$. Puisque le déterminant d'une matrice élémentaire n'est pas nul, on en déduit $\det P\neq 0$. Il vient donc $\det A=\det(AB)=0$ et l'on a bien l'égalité $\det(AB)=(\det A)(\det B)$. ∎

**Théorème.** *Une matrice $A$ de $M_n(\mathbf{K})$ est inversible si et seulement si son déterminant est non nul. De plus, si $A$ est inversible, alors $\det(A^{-1})=1/\det A$.*

**Démonstration.** C'est clair si $n=1$. Supposons $n\geqslant 2$. Nous venons de prouver, dans la démonstration du théorème précédent, que si $A$ n'est pas inversible, alors $\det A=0$. Supposons $A$ inversible. On a $A=P_1\cdots P_r$ où $P_i$ est une matrice élémentaire. Il vient $\det A=(\det P_1)\cdots(\det P_r)$. Puisque le déterminant d'une matrice élémentaire n'est pas nul, on en déduit $\det A\neq 0$. De plus, on a $1=\det I_n=\det(AA^{-1})=(\det A)(\det(A^{-1}))$. ∎

Ce théorème permet donc de savoir si une matrice carrée est inversible en calculant son déterminant.

**Exemple.** La matrice $\begin{bmatrix} a & b\\ c & d\end{bmatrix}$ est inversible si et seulement si $ad-bc\neq 0$.

**Proposition.** *Si $A$ est une matrice de $M_n(\mathbf{K})$, alors on a* $\det({}^tA)=\det A$.

**Démonstration.** Si $n=1$, alors ${}^tA=A$, donc $\det({}^tA)=\det A$. Supposons $n\geqslant 2$. Si $A$ est une matrice élémentaire de la forme $D_i(a)$, alors ${}^tA=A$, donc $\det({}^tA)=\det A$. Si $A$ est une matrice élémentaire de la forme $T_{ij}(\lambda)$, alors ${}^tA=T_{ji}(\lambda)$, donc $\det({}^tA)=\det A=1$. Puisque toute matrice inversible est produit de matrices élémentaires, on en déduit le résultat pour toute matrice inversible en raisonnant par récurrence. Supposons $A$ non inversible. Puisque ${}^t({}^tA)=A$ et que la transposée d'une matrice inversible est inversible, on en déduit que ${}^tA$ n'est pas inversible. D'après le théorème précédent, on a donc $\det A=\det({}^tA)=0$. ∎

Grâce à la proposition précédente, chacune des propriétés du déterminant relative aux lignes de la matrice fournit, en utilisant la transposée, une propriété relative aux colonnes :



- si on multiplie une colonne par $a$, alors le déterminant est multiplié par $a$
- si on échange deux colonnes, alors le déterminant est multiplié par $-1$
- si $A$, $A'$ et $A''$ sont des matrices qui ne diffèrent que par la $j$-ième colonne et si la $j$-ième colonne de $A$ est la somme de celles de $A'$ et $A''$, alors on a $\det A=\det A'+\det A''$
- si deux colonnes sont égales, alors le déterminant est nul
- le déterminant ne change pas lorsqu'on ajoute à une colonne $\lambda$ fois une autre.

**Exemple.** Pour tous nombres $x,y,z,x',y',z',\lambda$ appartenant à $\mathbf{K}$, on a

$$\begin{vmatrix} 1 & \lambda x+x' & 0\\ 2 & \lambda y+y' & 1\\ 1 & \lambda z+z' & 1\end{vmatrix}=\lambda\begin{vmatrix} 1 & x & 0\\ 2 & y & 1\\ 1 & z & 1\end{vmatrix}+\begin{vmatrix} 1 & x' & 0\\ 2 & y' & 1\\ 1 & z' & 1\end{vmatrix}.$$

Dans la définition du déterminant, la première colonne de la matrice joue un rôle privilégié : c'est la première colonne que l'on raye pour effectuer le calcul. La proposition suivante montre qu'on peut faire jouer un rôle analogue à n'importe quelle colonne et même à n'importe quelle ligne.

**Proposition.** *Supposons $n$ supérieur ou égal à 2. Soit $A=[a_{ij}]$ une matrice de $M_n(\mathbf{K})$. Si $\Delta_{k\ell}$ est le déterminant de la matrice de $M_{n-1}(\mathbf{K})$ obtenue à partir de $A$ en rayant la ligne $k$ et la colonne $\ell$, alors pour tous entiers $i,j\in\{1,2,\dots,n\}$, on a*

$$\det A=(-1)^{i+1}\left(a_{i1}\Delta_{i1}-a_{i2}\Delta_{i2}+\cdots+(-1)^{n+1}a_{in}\Delta_{in}\right)$$
$$\det A=(-1)^{j+1}\left(a_{1j}\Delta_{1j}-a_{2j}\Delta_{2j}+\cdots+(-1)^{n+1}a_{nj}\Delta_{nj}\right).$$

Si l'on choisit $j=1$ dans la seconde formule, on retrouve la définition du déterminant. Utiliser la première formule pour calculer le déterminant de $A$ s'appelle *développer le déterminant de $A$ selon* la $i$-ième ligne et utiliser la seconde formule s'appelle *développer le déterminant de $A$ selon* la $j$-ième colonne.

Ajouter $\lambda$ fois une ligne à une autre, ou bien ajouter $\lambda$ fois une colonne à une autre ne change pas le déterminant. Il faut utiliser ces propriétés pour calculer un déterminant : cela rend le calcul plus simple, plus rapide et plus sûr.

Pour calculer un déterminant, vous devez :
- choisir une ligne (ou une colonne) qui a le plus de 0
- si cela est possible, augmenter le nombre de ces 0 par opérations élémentaires sur les colonnes (ou sur les lignes)
- développer le déterminant selon cette ligne (ou colonne), sans oublier l'alternance des signes.

**Remarque**
Pour savoir par quel signe il faut commencer quand on développe un déterminant selon une ligne ou une colonne, on peut remplir un tableau à $n$ lignes et $n$ colonnes avec des signes : les signes sont alternés et on commence en haut à gauche par un signe $+$. Par exemple, voici les dessins correspondants lorsque $n$ est égal à 3, 4 ou 5.

$$\begin{bmatrix} + & - & + \\ - & + & - \\ + & - & + \end{bmatrix} \quad \begin{bmatrix} + & - & + & - \\ - & + & - & + \\ + & - & + & - \\ - & + & - & + \end{bmatrix} \quad \begin{bmatrix} + & - & + & - & + \\ - & + & - & + & - \\ + & - & + & - & + \\ - & + & - & + & - \\ + & - & + & - & + \end{bmatrix}$$

**Exemple.** Soient $a, x$ des nombres réels et $A$ la matrice de $M_4(\mathbf{R})$ définie par

$$A = \begin{bmatrix} x+1 & -2 & 2 & -2 \\ a & x-a-1 & a & -a \\ -2 & 2 & x-3 & 2 \\ -1 & 1 & -1 & x \end{bmatrix}.$$

Pour calculer le déterminant de $A$, ajoutons la troisième colonne à la dernière. Puisque cette opération ne change pas le déterminant, il vient

$$\det A = \begin{vmatrix} x+1 & -2 & 2 & 0 \\ a & x-a-1 & a & 0 \\ -2 & 2 & x-3 & x-1 \\ -1 & 1 & -1 & x-1 \end{vmatrix}.$$

Ensuite, retranchons la dernière ligne à la troisième et développons le déterminant obtenu selon la dernière colonne. On obtient

$$\det A = \begin{vmatrix} x+1 & -2 & 2 & 0 \\ a & x-a-1 & a & 0 \\ -1 & 1 & x-2 & 0 \\ -1 & 1 & -1 & x-1 \end{vmatrix} = (x-1) \begin{vmatrix} x+1 & -2 & 2 \\ a & x-a-1 & a \\ -1 & 1 & x-2 \end{vmatrix}.$$

Pour calculer le déterminant en facteur de $(x-1)$, ajoutons la deuxième colonne à la première, puis retranchons la première ligne à la deuxième. Il vient

$$\det A = (x-1) \begin{vmatrix} x-1 & -2 & 2 \\ x-1 & x-a-1 & a \\ 0 & 1 & x-2 \end{vmatrix} = (x-1) \begin{vmatrix} x-1 & -2 & 2 \\ 0 & x-a+1 & a-2 \\ 0 & 1 & x-2 \end{vmatrix}.$$

Enfin, en développant ce dernier déterminant selon la première colonne, on obtient

$$\det A = (x-1)^2 \begin{vmatrix} x-a+1 & a-2 \\ 1 & x-2 \end{vmatrix} = (x-1)^2(x^2 - x - ax + a),$$

c'est-à-dire $\det A = (x-1)^3(x-a)$.





## 3. Utilisation du déterminant

Au paragraphe précédent, nous avons démontré qu'une matrice carrée est inversible si et seulement si son déterminant est non nul. Voici des applications de ce résultat.

**Exercice.** Soient $a, b, c$ des nombres réels. Pour quelles valeurs du nombre réel $m$ existe-il des nombres réels $x, y, z$ uniques tels que $\begin{cases} mx - y + z = a \\ -x + my + z = b \\ x + y + mz = c \end{cases}$ ?

**Réponse.** La matrice de ce système est $A = \begin{bmatrix} m & -1 & 1 \\ -1 & m & 1 \\ 1 & 1 & m \end{bmatrix}$. Le système a une unique solution si et seulement si $A$ est inversible, c'est-à-dire si seulement si $\det A \neq 0$. Calculons le déterminant de $A$. Pour cela, ajoutons la troisième ligne à la deuxième, puis retranchons $m$ fois la troisième ligne à la première. Il vient

$$\det A = \begin{vmatrix} m & -1 & 1 \\ -1 & m & 1 \\ 1 & 1 & m \end{vmatrix} = \begin{vmatrix} m & -1 & 1 \\ 0 & m+1 & m+1 \\ 1 & 1 & m \end{vmatrix} = \begin{vmatrix} 0 & -1-m & 1-m^2 \\ 0 & m+1 & m+1 \\ 1 & 1 & m \end{vmatrix}.$$

Développons ce dernier déterminant selon la première colonne, puis mettons $m+1$ en facteur dans chaque ligne. On obtient

$$\det A = \begin{vmatrix} -1-m & 1-m^2 \\ m+1 & m+1 \end{vmatrix} = (m+1)^2 \begin{vmatrix} -1 & 1-m \\ 1 & 1 \end{vmatrix} = (m+1)^2(m-2).$$

Le système a donc une unique solution si et seulement si $m \neq -1$ et $m \neq 2$.

Nous allons maintenant montrer que lorsqu'un système d'équations linéaires a une solution unique, celle-ci peut s'exprimer au moyen de déterminants. Introduisons d'abord une notion commode pour ce genre de calculs : elle fait intervenir les nombres $\Delta_{ij}$ introduits dans la proposition page 89.

**Définition**
Soit $A = [a_{ij}]$ une matrice de $M_n(\mathbf{K})$, où $n \geqslant 2$. Notons $\Delta_{ij}$ le déterminant de la matrice de $M_{n-1}(\mathbf{K})$ obtenue à partir de $A$ en rayant la ligne $i$ et la colonne $j$. On appelle *cofacteur* de $a_{ij}$ le nombre $(-1)^{i+j}\Delta_{ij}$. La *comatrice* de $A$ est la matrice de $M_n(\mathbf{K})$ notée $\operatorname{Com} A$ dont le coefficient à l'intersection de la ligne $i$ et de la colonne $j$ est $(-1)^{i+j}\Delta_{ij}$.

Par exemple, si $A = \begin{bmatrix} 1 & 2 & 0 \\ 0 & 3 & 1 \\ 1 & 1 & 1 \end{bmatrix}$, alors

$$\operatorname{Com} A = \begin{bmatrix} \Delta_{11} & -\Delta_{12} & \Delta_{13} \\ -\Delta_{21} & \Delta_{22} & -\Delta_{23} \\ \Delta_{31} & -\Delta_{32} & \Delta_{33} \end{bmatrix} = \begin{bmatrix} 2 & 1 & -3 \\ -2 & 1 & 1 \\ 2 & -1 & 3 \end{bmatrix}.$$

**Proposition.** *Supposons $n$ supérieur ou égal à 2. Si $A$ est une matrice de $M_n(\mathbf{K})$, alors on a ${}^t(\mathrm{Com}\,A)A = A^t(\mathrm{Com}\,A) = (\det A)I_n$.*

**Démonstration abrégée.** Posons $B = {}^t(\mathrm{Com}\,A)A$, $C = A^t(\mathrm{Com}\,A)$ et reprenons les notations de la définition ci-dessus. Si $B = [b_{ij}]$ et $C = [c_{ij}]$, alors par définition du produit matriciel, on a

$$b_{11} = \Delta_{11}a_{11} - \Delta_{21}a_{21} + \cdots + (-1)^{n+1}\Delta_{n1}a_{n1}$$
$$b_{12} = -\Delta_{11}a_{12} + \Delta_{21}a_{22} - \cdots + (-1)^{n}\Delta_{n1}a_{n2}$$
$$c_{11} = a_{11}\Delta_{11} - a_{12}\Delta_{12} + \cdots + (-1)^{n+1}a_{1n}\Delta_{1n}.$$

En développant le déterminant de $A$ selon la première colonne, on trouve $\det A = b_{11}$. Si on le développe selon la première ligne, on obtient $\det A = c_{11}$.

Notons $D$ la matrice de $M_n(\mathbf{K})$ dont toutes les colonnes sauf la première sont celles de $A$ et dont la première colonne est égale à la deuxième de $A$. Puisque la matrice $D$ a ses deux premières colonnes égales, on a $\det D = 0$. Mais si nous développons le déterminant de $D$ selon la première colonne, nous obtenons $\det D = -b_{12}$. Il s'ensuit $b_{12} = 0$. On démontre de la même manière que l'on a $b_{ij} = c_{ij} = 0$ si $i \neq j$ et $b_{ii} = c_{ii} = \det A$. ∎

**Corollaire.** *Supposons $n$ supérieur ou égal à 2. Si $A$ est une matrice inversible de $M_n(\mathbf{K})$, alors on a $A^{-1} = \dfrac{1}{\det A}\,{}^t(\mathrm{Com}\,A)$.*

Ce corollaire a un intérêt théorique et sert assez peu dans la pratique, sauf si $n = 2$. En effet, si $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, alors ${}^t(\mathrm{Com}\,A) = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$. Si $ad - bc \neq 0$, on a donc

$$A^{-1} = \frac{1}{ad - bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Cette dernière formule est utile pour résoudre un système à deux équations et à deux inconnues dont la matrice est inversible.

**Proposition.** *Supposons $n$ supérieur ou égal à 2. Soient $A$ une matrice inversible de $M_n(\mathbf{K})$ et $B$ une matrice de $M_{n,1}(\mathbf{K})$. Si l'on note $M_i$ la matrice de $M_n(\mathbf{K})$ dont la $i$-ième colonne est $B$ et dont toutes les autres colonnes sont celles de $A$, alors la solution du système d'équations linéaires $AX = B$ est la matrice de $M_{n,1}(\mathbf{K})$ dont le coefficient de la $i$-ième ligne est égal à $(\det M_i)/(\det A)$.*

**Démonstration abrégée.** Puisque la matrice $A$ est inversible, le système d'équations linéaires $AX = B$ a une unique solution : la matrice $A^{-1}B = (1/\det A)C$, où l'on a posé $C = {}^t(\mathrm{Com}\,A)B$. Notons $c_i$ le coefficient de la $i$-ième ligne de la matrice-colonne $C$. Par définition du produit matriciel, il vient $c_1 = \Delta_{11}b_1 - \Delta_{21}b_2 + \cdots + (-1)^{n+1}\Delta_{n1}b_n$. D'autre part, en développant le déterminant de $M_1$ selon la première colonne, on trouve $c_1 = \det M_1$. De même, en développant le déterminant de $M_i$ selon la $i$-ième colonne, on trouve $c_i = \det M_i$. Le coefficient de la $i$-ième ligne de $A^{-1}B$ est donc bien égal à $(\det M_i)/(\det A)$. ∎





Les formules de la proposition ci-dessus s'appellent les *formules de Cramer*.

**Exercice**

a) Pour tous nombres $a, b, c$ de $\mathbf{K}$, calculer le déterminant de la matrice

$$\begin{bmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 & b^2 & c^2 \end{bmatrix}.$$

b) Soient $a, b, c, d$ des nombres de $\mathbf{K}$. On suppose que $a, b, c$ sont deux à deux différents. Montrer qu'il existe des nombres $x, y, z$ uniques tels que

$$\begin{cases} x + y + z = d \\ ax + by + cz = d^2 \\ a^2x + b^2y + c^2z = d^3. \end{cases}$$

Calculer ces nombres $x, y, z$.

**Réponse**

a) Pour calculer le déterminant de la matrice, retranchons la première colonne à la deuxième et à la troisième. Il vient

$$\begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 & b^2 & c^2 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 \\ a & b-a & c-a \\ a^2 & b^2-a^2 & c^2-a^2 \end{vmatrix} = (b-a)(c-a)\begin{vmatrix} 1 & 0 & 0 \\ a & 1 & 1 \\ a^2 & b+a & c+a \end{vmatrix}.$$

En développant ce dernier déterminant selon la première ligne, on obtient

$$\begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 & b^2 & c^2 \end{vmatrix} = (b-a)(c-a)\begin{vmatrix} 1 & 1 \\ b+a & c+a \end{vmatrix} = (b-a)(c-a)(c-b).$$

b) Puisque les nombres $a$, $b$ et $c$ sont deux à deux différents, la matrice du système que l'on cherche à résoudre a un déterminant non nul, donc est inversible. Il s'ensuit que le système a une unique solution. D'après les formules de Cramer, cette solution est

$$\begin{cases} x = \dfrac{M_1}{(b-a)(c-a)(c-b)} \\ y = \dfrac{M_2}{(b-a)(c-a)(c-b)} \\ z = \dfrac{M_3}{(b-a)(c-a)(c-b)}, \end{cases}$$

où l'on a

$$M_1 = \begin{vmatrix} d & 1 & 1 \\ d^2 & b & c \\ d^3 & b^2 & c^2 \end{vmatrix}, \quad M_2 = \begin{vmatrix} 1 & d & 1 \\ a & d^2 & c \\ a^2 & d^3 & c^2 \end{vmatrix} \quad \text{et} \quad M_3 = \begin{vmatrix} 1 & 1 & d \\ a & b & d^2 \\ a^2 & b^2 & d^3 \end{vmatrix}.$$

En utilisant la première question (en remplaçant la lettre $a$ par la lettre $d$), il vient

$$M_1 = d\begin{vmatrix} 1 & 1 & 1 \\ d & b & c \\ d^2 & b^2 & c^2 \end{vmatrix} = d(b-d)(c-d)(c-b).$$

De même, il vient $M_2 = d(d-a)(c-a)(c-d)$ et $M_3 = d(b-a)(d-a)(d-b)$. On en déduit que l'unique solution cherchée est

$$\begin{cases} x = \dfrac{d(b-d)(c-d)}{(b-a)(c-a)} \\ y = \dfrac{d(d-a)(c-d)}{(b-a)(c-b)} \\ z = \dfrac{d(d-a)(d-b)}{(c-a)(c-b)} \end{cases}.$$

## Exercices

**1.** Pour tous nombres $a, b, c, d$ de $\mathbf{K}$, calculer le déterminant $\begin{vmatrix} a & 1 & 0 & 2 \\ 0 & b & 0 & 3 \\ 4 & 5 & c & 6 \\ 0 & 0 & 0 & d \end{vmatrix}$.

**2.** Soit $x$ un nombre de $\mathbf{K}$. Calculer le déterminant

$$\begin{vmatrix} 1+x & 1 & 1 & 1 & 1 \\ 1 & 1+x & 1 & 1 & 1 \\ 1 & 1 & 1+x & 1 & 1 \\ 1 & 1 & 1 & 1+x & 1 \\ 1 & 1 & 1 & 1 & 1+x \end{vmatrix}.$$

**3.** La matrice $\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \\ 1 & -i & -1 & i \end{bmatrix}$ de $M_4(\mathbf{C})$ est-elle inversible ?

**4.** La matrice $\begin{bmatrix} 2 & 1 & 0 & 0 & 0 \\ 2 & 2 & 1 & 0 & 0 \\ 2 & 3 & 2 & 1 & 0 \\ 2 & 4 & 3 & 2 & 1 \\ 2 & 5 & 4 & 3 & 2 \end{bmatrix}$ de $M_5(\mathbf{Q})$ est-elle inversible ?



**5.** Soient $x, y, z, t, u, v$ des nombres de $K$. Montrer que l'on a

$$\begin{vmatrix} 0 & x & y & z \\ -x & 0 & t & u \\ -y & -t & 0 & v \\ -z & -u & -v & 0 \end{vmatrix} = (xv - yu + zt)^2.$$

**6.** Pour quelles valeurs du nombre réel $a$ existe-il des nombres réels $x, y, z$ uniques tels que

$$\begin{cases} x + 2y + z = 1 \\ 2x + (a+3)y + 3z = 2 \\ x + (3-a)y + (a-2)z = 3 \end{cases} ?$$

**7.** Soit $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ une matrice de $M_2(\mathbf{K})$. On définit la *trace* de la matrice $A$ comme étant le nombre $\operatorname{tr} A = a + d$.

**a)** Calculer la matrice $A^2 - (\operatorname{tr} A)A + (\det A)I_2$.

**b)** On suppose la matrice $A$ inversible. Montrer que la matrice $A^{-1}$ est combinaison linéaire de $I_2$ et $A$.

**8.** Soit $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ une matrice de $M_2(\mathbf{R})$. La trace de $A$ est le nombre $\operatorname{tr} A = a + d$.

**a)** Montrer que si $A^2 = -I_2$, alors $\operatorname{tr} A = 0$.

**b)** Montrer qu'on a l'égalité $A^2 = -I_2$ si et seulement si $\operatorname{tr} A = 0$ et $\det A = 1$.

**c)** Trouver une matrice $B$ de $M_2(\mathbf{R})$ telle que $B^2 = -I_2$.

**d)** Trouver une matrice $C$ de $M_2(\mathbf{C})$ telle que $C^2 = -I_2$ et $\operatorname{tr} C \neq 0$.

**9.** Posons $\Delta_2 = \begin{vmatrix} 2 & -1 \\ -1 & 2 \end{vmatrix}$, $\Delta_3 = \begin{vmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 2 \end{vmatrix}$, $\Delta_4 = \begin{vmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & -1 & 0 \\ 0 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{vmatrix}$

$$\text{et} \quad \Delta_n = \begin{vmatrix} 2 & -1 & 0 & \cdots & 0 \\ -1 & \ddots & \ddots & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & -1 \\ 0 & \cdots & 0 & -1 & 2 \end{vmatrix} \quad \text{si} \quad n \geqslant 5.$$

**a)** Calculer $\Delta_2$ et $\Delta_3$.

**b)** Montrer que pour tout $n \geqslant 2$, on a $\Delta_{n+2} = 2\Delta_{n+1} - \Delta_n$.

**c)** Montrer que pour tout $n \geqslant 2$, on a $\Delta_n = n + 1$.

**10.** Soit $A \in M_3(\mathbb{Q})$ la matrice définie par $A = \begin{bmatrix} 2 & 1 & -1 \\ -1 & 2 & 1 \\ -1 & 1 & 2 \end{bmatrix}$.

**a)** Pour quelles valeurs du nombre rationnel $\lambda$ la matrice $A - \lambda I_3$ est-elle inversible ? Dans ce cas, calculer l'inverse de $A - \lambda I_3$.

**b)** Soit $\lambda \in \mathbb{Q}$. On suppose $A - \lambda I_3$ non inversible. Trouver toutes les matrices $X \in M_{3,1}(\mathbb{Q})$ telles que $AX = \lambda X$.

**11.** Soient $n$ un entier au moins égal à 2 et $A$ une matrice de $M_n(\mathbf{K})$. Soit $p$ un entier compris entre 1 et $n$.

**a)** Supposons que dans la $p$-ième colonne de $A$, tous les coefficients sont nuls sauf celui de la $p$-ième ligne qui vaut 1. Trouver une matrice-colonne $X$ non nulle telle que $AX = X$.

**b)** Supposons que dans la $p$-ième ligne de $A$, tous les coefficients sont nuls sauf celui de la $p$-ième colonne qui vaut 1. Montrer qu'il existe une matrice-colonne $X$ non nulle telle que $AX = X$.

**12.** Soient $x_1, x_2, x_3, y_1, y_2, y_3$ des nombres de $\mathbf{K}$. Calculer le déterminant

$$\begin{vmatrix} 1 + x_1y_1 & 1 + x_1y_2 & 1 + x_1y_3 \\ 1 + x_2y_1 & 1 + x_2y_2 & 1 + x_2y_3 \\ 1 + x_3y_1 & 1 + x_3y_2 & 1 + x_3y_3 \end{vmatrix}.$$

**13.** Soient $n$ un entier supérieur ou égal à 2 et $A$ une matrice de $M_n(\mathbf{K})$.

**a)** Exprimer $\det(-A)$ en fonction de $\det A$.

**b)** On suppose que $n$ est impair et que l'on a ${}^tA = -A$. Montrer que $\det A = 0$.

**14.** Montrer qu'il n'existe pas de matrice $A \in M_3(\mathbb{R})$ telle que $A^2 = -I_3$.

## Quelques réponses ou indications

2. Ajouter par exemple les quatre dernières lignes à la première, retrancher la première colonne à toutes les autres et développer selon la première ligne. Le déterminant est égal à $x^4(5+x)$.

6. La condition est que la matrice du système soit inversible, ce qui a lieu si et seulement si $a$ est différent de 1 et 2.

7. **a)** On a l'égalité $A^2 - (\operatorname{tr} A)A + (\det A)I_2 = 0$.
**b)** On a $A(A - (\operatorname{tr} A)I_2) = A^2 - (\operatorname{tr} A)A = (-\det A)I_2$ et $\det A \neq 0$.

8. **a)** Ne pas oublier que la matrice $A$ est à coefficients réels.
**b)** On peut utiliser l'égalité $A^2 - (\operatorname{tr} A)A + (\det A)I_2 = 0$ démontrée dans l'exercice précédent ou bien raisonner directement.



10. **a)** La matrice $A - \lambda I_3$ est inversible si et seulement si $\lambda \neq 1, 2, 3$.
**b)** Puisqu'on a $(A - \lambda I_3)X = AX - \lambda X$, il faut résoudre le système $(A - \lambda I_3)X = 0$ pour chacune des valeurs $\lambda = 1, 2$ ou 3.

11. **a)** L'hypothèse signifie que la $p$-ième colonne de la matrice $A$ est $E_p$ (les matrices $E_i$ ont été définies au chapitre précédent).
**b)** L'égalité $AX = X$ est équivalente au système d'équations $(A - I_n)X = 0$.

12. Retrancher par exemple la première colonne à la deuxième et à la troisième. Le déterminant est égal à 0.

13. **a)** On a $\det(-A) = (-1)^n \det A$.

14. Considérer le déterminant de chaque membre.

# Chapitre 6

# Espaces vectoriels

Comme vous allez le voir, vous connaissez déjà certains *espaces vectoriels* et vous savez calculer dans ceux-ci. Les règles de calcul que nous allons présenter ne seront donc pas nouvelles. Il est cependant nécessaire de les formaliser pour définir la notion même d'espace vectoriel. Dans ce chapitre, la lettre $\mathbf{K}$ désigne $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ et les éléments de $\mathbf{K}$ seront souvent appelés des *scalaires*.

## 1. Règles de calcul

Un $\mathbf{K}$-*espace vectoriel*, ou un *espace vectoriel sur* $\mathbf{K}$, est un ensemble non vide $E$ dont les éléments s'appellent des *vecteurs* et qui est muni de deux opérations, la somme de vecteurs et la multiplication d'un vecteur par un scalaire, vérifiant un certain nombre de propriétés.

La somme des vecteurs $x$ et $y$ de $E$ est le vecteur de $E$ noté $x+y$. De plus, si $\lambda$ est un élément de $\mathbf{K}$, la multiplication du vecteur $x$ par le scalaire $\lambda$ est le vecteur de $E$ noté $\lambda x$.

Les règles de calcul sont les suivantes :

- pour tous $x, y \in E$, on a $x+y=y+x$
- pour tous $x, y, z \in E$, on a $(x+y)+z=x+(y+z)$ et ce vecteur est noté $x+y+z$
- il existe un vecteur $e \in E$ tel que $x+e=x$ pour tout $x \in E$ ; de plus, pour tout $y \in E$, il existe un vecteur $y' \in E$ tel que $y+y'=e$
- pour tout $x \in E$, on a $1x=x$
- pour tout $x \in E$ et pour tous $\lambda, \mu \in \mathbf{K}$, on a $(\lambda+\mu)x=\lambda x+\mu x$ et $(\lambda\mu)x=\lambda(\mu x)$, ce dernier vecteur étant noté $\lambda\mu x$
- pour tous $x, y \in E$ et pour tout $\lambda \in \mathbf{K}$, on a $\lambda(x+y)=\lambda x+\lambda y$.

L'élément $e$ défini ci-dessus est nécessairement ***unique***. En effet, si $e' \in E$ vérifie également $x+e'=x$ pour tout $x \in E$, il vient $e+e'=e$ et $e'+e=e'$. Puisque $e+e'=e'+e$, il s'ensuit $e=e'$. Cet unique vecteur de $E$ s'appelle le *vecteur nul* de

$E$ et se note 0, par analogie avec le calcul sur les nombres de **K**. La règle de calcul correspondante s'écrit donc $x + 0 = x$ pour tout $x \in E$.

Grâce à la deuxième règle de calcul, on en déduit que pour tout $y \in E$, il existe un *unique* $y' \in E$ tel que $y + y' = 0$. En effet, si $y''$ est un autre vecteur tel que $y + y'' = 0$, il vient $y'' = 0 + y'' = y + y' + y'' = y + y'' + y' = 0 + y' = y'$.

**Proposition.** *Soit $E$ un espace vectoriel sur* **K**.

- *Pour tous $x, y, z \in E$, si l'on a $x + z = y + z$, alors $x = y$.*
- *Pour tout $x \in E$, on a $0x = 0$ et pour tout $\lambda \in$ **K**, on a $\lambda 0 = 0$.*
- *Pour tous $x \in E$ et $\lambda \in$ **K**, si $\lambda x = 0$, alors $\lambda = 0$ ou $x = 0$.*

**Démonstration.** Si l'on a $x + z = y + z$, on ajoute à chaque membre de cette égalité l'unique vecteur $z' \in E$ tel que $z + z' = 0$ ; il vient $x + 0 = y + 0$, c'est-à-dire $x = y$. Pour tout $x \in E$, on a $x + 0 = x = 1x = (1 + 0)x = 1x + 0x = x + 0x$. Il s'ensuit $0x = 0$. Pour tout $\lambda \in$ **K**, on a $\lambda 0 + \lambda 0 = \lambda(0 + 0) = \lambda 0 = \lambda 0 + 0$, d'où $\lambda 0 = 0$. Soient $x \in E$ et $\lambda \in$ **K** tels que $\lambda x = 0$. Si $\lambda \neq 0$, alors le scalaire $\mu = 1/\lambda$ est bien défini et l'on a $0 = \mu(\lambda x) = (\mu\lambda)x = 1x = x$. ∎

**Notation.** Si $x \in E$, le vecteur $(-1)x$ est noté $-x$. De plus, si $y \in E$, le vecteur $y + (-x)$ est noté $y - x$. Nous avons alors $x - x = (1 - 1)x = 0x = 0$ pour tout $x \in E$.

### Conséquences des règles de calcul

- Pour tous vecteurs $y$ et $y'$ appartenant à $E$, nous avons les équivalences

$$y + y' = 0 \iff y' = -y \iff y = -y'.$$

- Pour tous vecteurs $y$ et $y'$ appartenant à $E$ et pour tout scalaire $\lambda$ non nul, on a l'équivalence

$$\lambda y = y' \iff y = (1/\lambda)y'.$$

En effet, étant donné un vecteur $y$, il n'y a qu'un seul vecteur $y'$ tel que $y + y' = 0$ et le vecteur $y' = -y$ satisfait à cette égalité. Pour la seconde affirmation, on remarque que si $\lambda y = y'$, alors en multipliant par le scalaire $(1/\lambda)$ (qui existe puisque $\lambda$ est différent de 0), on a $(1/\lambda)y' = (1/\lambda)(\lambda y) = ((1/\lambda)\lambda)y = 1y = y$.

### Exemples

- L'ensemble **K** lui-même est un **K**-espace vectoriel. L'addition et la multiplication par un scalaire sont les opérations d'addition et de multiplication dans **K**.
- L'ensemble **R** est un **Q**-espace vectoriel. La multiplication du vecteur $x \in$ **R** par le scalaire $\lambda \in$ **Q** est simplement le produit des deux nombres réels $\lambda$ et $x$.
- De même, **C** est un **R**-espace vectoriel et aussi un **Q**-espace vectoriel.





- L'ensemble des matrices $n \times p$ à coefficients dans **K** est un espace vectoriel sur **K**. Les opérations somme et multiplication par un scalaire sont celles qui ont été définies dans le chapitre 4. Quand on considérera l'espace vectoriel $M_{n,p}(\mathbf{K})$ sans préciser, il sera sous-entendu le **K**-espace vectoriel ainsi défini.
- Si $I$ est un intervalle de **R**, alors l'ensemble des fonctions de $I$ dans **R** est un **R**-espace vectoriel. Si $f : I \to \mathbf{R}$ et $g : I \to \mathbf{R}$, alors $f + g : I \to \mathbf{R}$ est la fonction définie par $(f + g)(x) = f(x) + g(x)$. De plus, si $\lambda \in \mathbf{R}$, alors $\lambda f : I \to \mathbf{R}$ est la fonction définie par $(\lambda f)(x) = \lambda f(x)$.
- L'ensemble des suites de nombres de **K** est un espace vectoriel sur **K**. C'est l'espace vectoriel des fonctions de **N** dans **K** : comme cela a été défini dans le tome d'Analyse, la somme de deux suites $(u_n)$ et $(v_n)$ est en effet la suite de terme général $u_n + v_n$ et le produit de la suite $(u_n)$ par le nombre $\lambda \in$ **K** est la suite de terme général $\lambda u_n$.

### Espace vectoriel produit

Si $A$ et $B$ sont des ensembles, rappelons que le produit cartésien $A \times B$ (voir chapitre 2) est l'ensemble des couples $(x, y)$, où $x$ décrit $A$ et où $y$ décrit $B$. Nous allons voir que si $E$ et $F$ sont des **K**-espaces vectoriels, alors $E \times F$ aussi. Il s'agit tout d'abord de définir la somme et la multiplication par un scalaire dans $E \times F$.

**Définition**

Soient $E$ et $F$ des **K**-espaces vectoriels. La somme des éléments $(x, y)$ et $(x', y')$ de $E \times F$ est définie par $(x, y) + (x', y') = (x + x', y + y')$ et le produit d'un élément $(x, y) \in E \times F$ par un scalaire $\lambda \in$ **K** est défini par $\lambda(x, y) = (\lambda x, \lambda y)$.

**Proposition.** *Soient $E$ et $F$ des* **K***-espaces vectoriels. Muni des opérations définies ci-dessus, $E \times F$ est un* **K***-espace vectoriel, appelé l'espace vectoriel produit de $E$ par $F$.*

Il est facile de vérifier que les règles de calcul imposées dans un espace vectoriel sont satisfaites dans $E \times F$. Indiquons juste que le vecteur nul de $E \times F$ est le vecteur dont chaque composante est nulle, c'est-à-dire $(0, 0)$ et que par commodité, on le note également 0.

Dans un espace vectoriel produit, on calcule composante par composante.

Si $n$ est un entier supérieur ou égal à 2, rappelons que l'on note $\mathbf{K}^n$ l'ensemble dont les éléments sont les $n$-uples $(a_1, \ldots, a_n)$, où les $a_i$ appartiennent à $\mathbf{K}$. Alors $\mathbf{K}^n$ est un $\mathbf{K}$-espace vectoriel. Remarquons que le vecteur nul de $\mathbf{K}^n$ est le vecteur $(0, \ldots, 0)$. Nous verrons au chapitre 7 que $\mathbf{K}^n$ est un exemple fondamental d'espace vectoriel.

**Définitions**

Soient $n$ un entier positif et $x_1, \ldots, x_n, y$ des vecteurs d'un $\mathbf{K}$-espace vectoriel.

- S'il existe $\lambda_1 \in \mathbf{K}$ tel que $y = \lambda_1 x_1$, alors on dit que le vecteur $y$ est *colinéaire* à $x_1$
- si $n \geqslant 2$ et s'il existe $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbf{K}$ tels que $y = \lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n$, alors on dit que le vecteur $y$ est *combinaison linéaire* de $x_1, \ldots, x_n$.

**Exemple.** Soient $f, g, h$ les éléments de l'espace vectoriel des fonctions de $\mathbb{R}$ dans $\mathbb{R}$, définis par $f(x) = \cos 2x$, $g(x) = (\sin x)^2$ et $h(x) = 1$ pour tout $x \in \mathbb{R}$. Puisqu'on a $\cos 2x = (\cos x)^2 - (\sin x)^2 = 1 - 2(\sin x)^2$, c'est-à-dire $f(x) = h(x) - 2g(x)$ pour tout $x \in \mathbb{R}$, on en déduit l'égalité $h = f + 2g$. Le vecteur $h$ est ainsi combinaison linéaire des vecteurs $f$ et $g$.

Pour simplifier la formulation des énoncés, nous serons amenés dans la suite de l'exposé à écrire que le vecteur $y$ est combinaison linéaire de $x_1, \ldots, x_n$, même lorsque $n = 1$. Dans ce cas, cela voudra dire que $y$ est colinéaire à $x_1$.

## 2. Sous-espaces vectoriels

Dans ce paragraphe, $E$ est un espace vectoriel sur $\mathbf{K}$.

**Définition**

Soit $F$ une partie de $E$. On dit que $F$ est un *sous-espace vectoriel* de $E$ si le vecteur nul de $E$ appartient à $F$, si pour tous $x, y \in F$, on a $x + y \in F$ et si pour tout $x \in F$ et pour tout $\lambda \in \mathbf{K}$, on a $\lambda x \in F$.

En raisonnant par récurrence, on démontre que si $n$ est un entier positif et si $x_1, \ldots, x_n$ sont des vecteurs d'un sous-espace vectoriel $F$ de $E$, alors toute combinaison linéaire de $x_1, \ldots, x_n$ appartient à $F$.

**Proposition.** *Tout sous-espace vectoriel de $E$ est un espace vectoriel sur $\mathbf{K}$.*

**Démonstration.** Soit $F$ un sous-espace vectoriel de $E$. Le vecteur nul de $E$ appartient à $F$ donc $F$ n'est pas vide. De plus, les opérations somme de deux vecteurs de $F$ et multiplication d'un vecteur de $F$ par un scalaire sont bien définies dans $F$, c'est-à-dire qu'elles prennent leurs valeurs dans $F$. Puisqu'on a $0 \in F$, $0$ est le vecteur de $F$ tel que $x + 0 = x$ pour tout $x \in F$ ; de plus, pour tout $y \in F$, on a $-y \in F$ et $-y$ est le vecteur de $F$ tel que $y + (-y) = 0$. Les autres règles de calcul sont automatiquement vérifiées dans $F$, puisqu'elles le sont dans $E$. Il s'ensuit que $F$ est un espace vectoriel sur $\mathbf{K}$. ∎





Cette proposition justifie la terminologie « sous-espace vectoriel ». Les sous-espaces vectoriels vont fournir de nouveaux et nombreux exemples d'espaces vectoriels.

**Exemples**

- Les parties $\{0\}$ et $E$ sont des sous-espaces vectoriels de $E$.
- Soit $I$ un intervalle de $\mathbb{R}$. La somme de deux fonctions continues sur $I$ est continue et si l'on multiplie par un nombre réel une fonction continue sur $I$, on obtient une fonction continue sur $I$. Puisque la fonction nulle est continue, l'ensemble des fonctions continues de $I$ dans $\mathbb{R}$ est un sous-espace vectoriel de l'espace vectoriel des fonctions de $I$ dans $\mathbb{R}$.
- L'ensemble des suites convergentes de nombres réels est un sous-espace vectoriel du $\mathbb{R}$-espace vectoriel des suites de nombres réels. En effet, d'après les propriétés des limites, la somme de deux suites convergentes est convergente et si l'on multiplie une suite convergente par un nombre réel, on obtient une suite convergente ; de plus, la suite dont tous les termes sont nuls est convergente.

**Proposition.** *Soient $n$ un entier supérieur ou égal à 2 et $a_1, a_2, \ldots, a_n \in \mathbf{K}$. Soit $F$ l'ensemble des vecteurs $(x_1, x_2, \ldots, x_n)$ de $\mathbf{K}^n$ tels que $a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0$. Alors $F$ est un sous-espace vectoriel de $\mathbf{K}^n$.*

**Démonstration.** Le vecteur nul de $\mathbf{K}^n$ appartient clairement à $F$. D'autre part, soient $x = (x_1, x_2, \ldots, x_n)$, $y = (y_1, y_2, \ldots, y_n)$ des vecteurs de $F$. Il vient

$$(a_1x_1 + a_2x_2 + \cdots + a_nx_n) + (a_1y_1 + a_2y_2 + \cdots + a_ny_n) = 0,$$
$$a_1(x_1 + y_1) + a_2(x_2 + y_2) + \cdots + a_n(x_n + y_n) = 0;$$

le vecteur $x + y = (x_1 + y_1, \ldots, x_n + y_n)$ appartient donc à $F$. De même, si $\lambda$ est un élément de $\mathbf{K}$, alors on a $\lambda(a_1x_1 + a_2x_2 + \cdots + a_nx_n) = 0$, ou encore $a_1(\lambda x_1) + a_2(\lambda x_2) + \cdots + a_n(\lambda x_n) = 0$ ; le vecteur $\lambda x = (\lambda x_1, \ldots, \lambda x_n)$ appartient donc à $F$. ∎

Si $F$ et $G$ sont des parties de $E$, rappelons que l'intersection $F \cap G$ est l'ensemble des éléments de $E$ qui appartiennent à la fois à $F$ et à $G$ (voir chapitre 2).

**Proposition.** *Si $F$ et $G$ sont des sous-espaces vectoriels de $E$, alors $F \cap G$ est un sous-espace vectoriel de $E$.*

**Démonstration.** Puisque le vecteur nul de $E$ appartient à $F$ et à $G$, il appartient à $F \cap G$. Soient $x$ et $y$ appartenant à $F \cap G$, c'est-à-dire à $F$ et à $G$. Puisque $F$ et $G$ sont des sous-espaces vectoriels de $E$, $x+y$ appartient à $F$ et à $G$, c'est-à-dire à $F \cap G$. De même, si $\lambda \in \mathbf{K}$, alors $\lambda x$ appartiennent à $F \cap G$. Il s'ensuit que $F \cap G$ est un sous-espace vectoriel de $E$. ∎

**Exemple.** L'ensemble des vecteurs $(x,y,z) \in \mathbb{R}^3$ tels que $\begin{cases} 2x+3y+4z=0 \\ -x+y+2z=0 \end{cases}$ est un sous-espace vectoriel de $\mathbb{R}^3$. En effet, c'est l'intersection des sous-espaces vectoriels $\{(x,y,z) \in \mathbb{R}^3 \mid 2x+3y+4z=0\}$ et $\{(x,y,z) \in \mathbb{R}^3 \mid -x+y+2z=0\}$ de $\mathbb{R}^3$.

De manière générale, l'ensemble des vecteurs $(x_1, x_2, \ldots, x_p)$ de $\mathbf{K}^p$ solutions du système d'équations linéaires

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1p}x_p = 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2p}x_p = 0 \\ \quad \vdots \qquad\qquad\qquad \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{np}x_p = 0 \end{cases}$$

est un sous-espace vectoriel de $\mathbf{K}^p$.

**Proposition.** *Soient $n$ un entier positif et $x_1, \ldots, x_n$ des vecteurs de $E$. Soit $F$ l'ensemble des vecteurs de $E$ qui sont combinaison linéaire de $x_1, \ldots, x_n$. Alors $F$ est un sous-espace vectoriel de $E$ et s'appelle le* sous-espace vectoriel de $E$ engendré *par les vecteurs $x_1, \ldots, x_n$.*

**Démonstration.** On a $0 = 0x_1 + \cdots + 0x_n$, par suite $0 \in F$. Soient $x, y \in F$. Par définition, il existe des scalaires $\lambda_1, \ldots, \lambda_n$ tels que $x = \lambda_1 x_1 + \cdots + \lambda_n x_n$ et il existe des scalaires $\mu_1, \ldots, \mu_n$ tels que $y = \mu_1 x_1 + \cdots + \mu_n x_n$. Il vient $x + y = (\lambda_1 + \mu_1)x_1 + \cdots + (\lambda_n + \mu_n)x_n$ et $\lambda x = (\lambda\lambda_1)x_1 + \cdots + (\lambda\lambda_n)x_n$ pour tout $\lambda \in \mathbf{K}$. Ainsi $x+y$ et $\lambda x$ sont combinaison linéaire de $x_1, \ldots, x_n$. Il s'ensuit que $F$ est un sous-espace vectoriel de $E$. ∎

**Exemple.** Soit $F = \{(x,y,z) \in \mathbb{R}^3 \mid x - 2y + z = 0\}$. Pour tous nombres réels $x, y, z$, nous avons les équivalences

$$\begin{aligned} x - 2y + z = 0 &\iff x = 2y - z \iff (x,y,z) = (2y - z, y, z) \\ &\iff (x,y,z) = y(2,1,0) + z(-1,0,1). \end{aligned}$$

On en déduit que $F$ est le sous-espace vectoriel de $\mathbb{R}^3$ engendré par les vecteurs $(2,1,0)$ et $(-1,0,1)$.

**Remarque**
Soit $F$ le sous-espace vectoriel de $E$ engendré par les vecteurs $x_1, \ldots, x_n$. S'il existe des vecteurs $y_1, \ldots, y_p$ de $F$ tels que, pour tout $i$, $x_i$ est combinaison linéaire de $y_1, \ldots, y_p$, alors $F$ est aussi le sous-espace vectoriel de $E$ engendré par les vecteurs $y_1, \ldots, y_p$.



En plus de l'intersection et de la notion de sous-espace vectoriel engendré par des vecteurs, voici une autre façon d'obtenir de nouveaux sous-espaces vectoriels.

**Proposition.** *Soient $F$ et $G$ des sous-espaces vectoriels de $E$ et soit $H$ l'ensemble des vecteurs $z \in E$ qui s'écrivent $z = x + y$, où $x \in F$ et $y \in G$. Alors $H$ est un sous-espace vectoriel de $E$. L'espace vectoriel $H$ s'appelle la* somme *de $F$ et $G$ et se note $F+G$.*

**Démonstration.** Il est clair que le vecteur nul de $E$ appartient à $H$. Soient $z, z' \in H$. Il existe $x, x' \in F$ et $y, y' \in G$ tels que $z = x + y$ et $z' = x' + y'$. Il vient $z + z' = (x+y) + (x'+y') = (x + x') + (y + y')$. Puisque $F$ et $G$ sont des sous-espaces vectoriels de $E$, on a $x + x' \in F$, $y + y' \in G$ et par suite $z + z' \in H$. De plus, pour tout $\lambda \in \mathbf{K}$, on a $\lambda z = \lambda x + \lambda y$, $\lambda x \in F$ et $\lambda y \in G$, donc $\lambda z \in H$. Il s'ensuit que $H$ est un sous-espace vectoriel de $E$. ∎

**Remarque**
Si $F$ et $G$ sont des sous-espaces vectoriels de $E$, alors on a $F \subset F+G$ et $G \subset F+G$. En effet, si $x \in F$, alors $x = x + 0$ et puisque $0 \in G$, on en déduit $x \in F+G$. Il s'ensuit que tout élément de $F$ appartient à $F+G$, par suite $F \subset F+G$. On démontre de même l'inclusion $G \subset F+G$.

**Proposition.** *Si $F$ est le sous-espace vectoriel de $E$ engendré par les vecteurs $x_1, \ldots, x_n$ et si $G$ est le sous-espace vectoriel de $E$ engendré par les vecteurs $y_1, \ldots, y_p$, alors $F+G$ est le sous-espace vectoriel de $E$ engendré par les vecteurs $x_1, \ldots, x_n, y_1, \ldots, y_p$.*

**Démonstration.** Les vecteurs $x_1, \ldots, x_n, y_1, \ldots, y_p$ appartiennent à $F$ ou à $G$ donc appartiennent tous à $F+G$, d'après la remarque précédente. Puisque $F+G$ est un sous-espace vectoriel de $E$, toute combinaison linéaire de ces vecteurs appartient à $F+G$. Réciproquement, si $z \in F+G$, alors il existe $x \in F$ et $y \in G$ tels que $z = x + y$. Puisque $x$ est combinaison linéaire de $x_1, \ldots, x_n$ et puisque $y$ combinaison linéaire de $y_1, \ldots, y_p$, le vecteur $z$ est combinaison linéaire de $x_1, \ldots, x_n, y_1, \ldots, y_p$. ∎

**Exemple.** Soient $F = \{(x,y,z) \in \mathbb{R}^3 \mid x+y+z=0\}$ et $G = \{(x,y,z) \in \mathbb{R}^3 \mid z = 0\}$. Pour tous nombres réels $x, y, z$, on a

$$x + y + z = 0 \iff (x,y,z) = (-y-z, y, z) = y(-1,1,0) + z(-1,0,1)$$

et

$$z = 0 \iff (x,y,z) = (x,y,0) = x(1,0,0) + y(0,1,0).$$

Il s'ensuit que $F$ est le sous-espace vectoriel de $\mathbb{R}^3$ engendré par les vecteurs $(-1,1,0)$ et $(-1,0,1)$, alors que $G$ est le sous-espace vectoriel de $\mathbb{R}^3$ engendré par les vecteurs

$(1,0,0)$ et $(0,1,0)$. Le sous-espace vectoriel $F+G$ est donc engendré par les vecteurs $(-1,1,0)$, $(-1,0,1)$, $(1,0,0)$ et $(0,1,0)$. Mais tout vecteur de $\mathbb{R}^3$ est combinaison linéaire des vecteurs $(-1,0,1)$, $(1,0,0)$ et $(0,1,0)$. En effet, pour tous $x,y,z\in\mathbb{R}$, il vient $(x,y,z)=(x+z)(1,0,0)+y(0,1,0)+z(-1,0,1)$. Tout vecteur de $\mathbb{R}^3$ est donc *a fortiori* combinaison linéaire des vecteurs $(-1,1,0)$, $(-1,0,1)$, $(1,0,0)$ et $(0,1,0)$. Il s'ensuit $F+G=\mathbb{R}^3$, autrement dit tout vecteur de $\mathbb{R}^3$ est somme d'un vecteur de $F$ et d'un vecteur de $G$.

Dans l'exemple précédent, on a $(1,1,1)=(0,-1,1)+(1,2,0)=(1,-2,1)+(0,3,0)$. Les vecteurs $(0,-1,1)$, $(1,-2,1)$ appartiennent à $F$ et les vecteurs $(1,2,0)$, $(0,3,0)$ appartiennent à $G$. Le vecteur $(1,1,1)$ s'écrit donc d'au moins deux manières différentes comme somme d'un vecteur de $F$ et d'un vecteur de $G$.

Nous allons voir que dans certains cas, ce phénomène est impossible. Formulons la définition correspondante.

**Définition**

Soient $F$ et $G$ des sous-espaces vectoriels de $E$. On dit que $F$ et $G$ sont *supplémentaires*, ou que $G$ est un *supplémentaire* de $F$, si tout vecteur de $E$ s'écrit de manière unique comme somme d'un vecteur de $F$ et d'un vecteur de $G$. Cette propriété se note $E=F\oplus G$.

**Proposition.** *Soient $F$ et $G$ des sous-espaces vectoriels de $E$. Les sous-espaces vectoriels $F$ et $G$ sont supplémentaires si et seulement si $E=F+G$ et $F\cap G=\{0\}$.*

**Démonstration.** Supposons $F$ et $G$ supplémentaires. En particulier, tout vecteur de $E$ est somme d'un vecteur de $F$ et d'un vecteur de $G$, par suite $E=F+G$. Puisque $F\cap G$ est un sous-espace vectoriel de $E$, on a $0\in F\cap G$. Si $x\in F\cap G$, on a $x=x+0=0+x$, $x\in F$ et $x\in G$, donc par unicité de la décomposition de $x$ en somme d'un vecteur de $F$ et d'un vecteur de $G$, on en déduit $x=0$. Nous avons donc $F\cap G=\{0\}$.

Réciproquement, supposons $E=F+G$ et $F\cap G=\{0\}$. Puisque $E=F+G$, tout vecteur de $E$ est somme d'un vecteur de $F$ et d'un vecteur de $G$. Soient $y,y'\in F$ et $z,z'\in G$ tels que $y+z=y'+z'$. Il vient $y-y'=z'-z$. Puisque $F$ et $G$ sont des sous-espaces vectoriels de $E$, on a $y-y'\in F$ et $z'-z\in G$. Il s'ensuit $y-y'\in F\cap G$, donc $y-y'=0$ et $z'-z=0$, c'est-à-dire $y=y'$ et $z=z'$. Tout vecteur de $E$ s'écrit donc de manière unique comme somme d'un vecteur de $F$ et d'un vecteur de $G$. Cela signifie que $F$ et $G$ sont supplémentaires. ∎

**Exemple.** Supposons que $E$ est le $\mathbb{R}$-espace vectoriel des fonctions de $\mathbb{R}$ dans $\mathbb{R}$. Soit $F$ l'ensemble des fonctions $f:\mathbb{R}\to\mathbb{R}$ telles que $f(x)=0$ pour tout $x\leqslant 0$. Pour toutes fonctions $f_1,f_2\in F$ et pour tout $x\leqslant 0$, on a $(f_1+f_2)(x)=f_1(x)+f_2(x)=0+0=0$.





Pour toute fonction $f\in F$ et pour tout $\lambda\in\mathbb{R}$, on a également $\lambda f\in F$. Il s'ensuit que $F$ est un sous-espace vectoriel de $E$, car la fonction nulle appartient à $F$.

De même, soit $G$ le sous-espace vectoriel de $E$ dont les éléments sont les fonctions $f:\mathbb{R}\to\mathbb{R}$ telles que $f(x)=0$ pour tout $x>0$.

Alors on a $E=F\oplus G$. En effet, pour toute fonction $f:\mathbb{R}\to\mathbb{R}$, notons $u:\mathbb{R}\to\mathbb{R}$ et $v:\mathbb{R}\to\mathbb{R}$ les fonctions définies par $u(x)=0$ si $x\leqslant 0$, $u(x)=f(x)$ si $x>0$, $v(x)=f(x)$ si $x\leqslant 0$ et $v(x)=0$ si $x>0$ ; alors on a $u\in F$, $v\in G$ et $f=u+v$. Il s'ensuit $E=F+G$. De plus, si $f\in F\cap G$, alors on a $f(x)=0$ pour tout $x\leqslant 0$ et pour tout $x>0$, donc $f$ est la fonction nulle. On en déduit $F\cap G=\{0\}$.

**Exercice.** Soit $E$ le $\mathbb{R}$-espace vectoriel des fonctions de $\mathbb{R}$ dans $\mathbb{R}$ et soit $F=\{f\in E \mid f(1)=f(2)\}$.

a) Montrer que $F$ est un sous-espace vectoriel de $E$.

b) Soit $g$ le vecteur de $E$ défini par $g(x)=x$ pour tout $x\in\mathbb{R}$ et soit $G$ le sous-espace vectoriel de $E$ engendré par $g$. Montrer que $F$ et $G$ sont supplémentaires.

**Réponse.**

a) La fonction nulle prend la valeur 0 en 1 et en 2, donc appartient à $F$. Soient $f$ et $h$ des vecteurs de $F$. Alors on a $f(1)=f(2)$ et $h(1)=h(2)$, donc $(f+h)(1)=f(1)+h(1)=f(2)+h(2)=(f+h)(2)$ ; le vecteur $f+h$ appartient donc à $F$. Si $\lambda$ est un nombre réel, on a $(\lambda f)(1)=\lambda f(1)=\lambda f(2)=(\lambda f)(2)$, donc le vecteur $\lambda f$ appartient à $F$.

b) Par définition, les vecteurs de $G$ sont les fonctions de la forme $\lambda g$, où $\lambda$ est un nombre réel. Soit $f$ un vecteur de $G$. Il existe donc un nombre réel $\lambda$ tel que $f=\lambda g$. Si $f$ appartient à $F$, alors il vient

$$0=f(2)-f(1)=(\lambda g)(2)-(\lambda g)(1)=\lambda g(2)-\lambda g(1)=\lambda(g(2)-g(1)=\lambda(2-1)=\lambda.$$

Ainsi nous avons $\lambda=0$, donc $f=\lambda g$ est la fonction nulle. Cela montre que l'ensemble $F\cap G$ est égal à $\{0\}$.

Soit $f\in E$. Cherchons à écrire $f$ comme la somme d'un vecteur de $F$ et d'un vecteur de $G$. Supposons que l'on ait $f=u+v$, où $u\in F$ et $v\in G$. Puisque $v\in G$, il existe un nombre réel $\lambda$ tel que $v=\lambda g$ et puisque $u\in F$, on doit avoir $u(1)=u(2)$. L'égalité de fonctions $f=u+v$ signifie que pour tout $x\in\mathbb{R}$, on a $f(x)=u(x)+v(x)$, donc il vient en particulier

$$f(1)=u(1)+v(1)=u(1)+\lambda g(1)=u(1)+\lambda$$
$$f(2)=u(2)+v(2)=u(2)+\lambda g(2)=u(2)+2\lambda.$$

En soustrayant la première égalité de la deuxième, on en déduit

$$f(2)-f(1)=u(2)-u(1)+\lambda=\lambda.$$

Définissons donc la fonction $v$ en posant $v=(f(2)-f(1))g$ et la fonction $u$ en posant $u=f-v$. Nous avons $v\in G$ et $f=u+v$. De plus, on a $v(2)-v(1)=(f(2)-f(1))(g(2)-g(1))=f(2)-f(1)$, donc $u(2)-u(1)=0$. Cela montre que $u$ appartient à $F$. Nous avons ainsi défini des vecteurs $u\in F$ et $v\in G$ tels que $f=u+v$, ce qui prouve que l'on a $E=F+G$.

## 3. Indépendance linéaire

Dans ce paragraphe, $E$ est un espace vectoriel sur $\mathbf{K}$.

**Définition**
Soient $n$ un entier positif et $x_1, \dots, x_n$ des vecteurs de $E$. Les vecteurs $x_1, \dots, x_n$ sont dits *linéairement indépendants* si pour tous $\lambda_1, \dots, \lambda_n \in \mathbf{K}$, on a l'implication

$$\lambda_1 x_1 + \cdots + \lambda_n x_n = 0 \Longrightarrow \lambda_1 = \cdots = \lambda_n = 0.$$

Ainsi les vecteurs $x_1, \dots, x_n$ sont linéairement indépendants s'il n'y a qu'une seule façon d'écrire le vecteur nul comme combinaison linéaire de $x_1, \dots, x_n$.

D'après la proposition page 100, un vecteur $x$ de $E$ est « linéairement indépendant » si et seulement si $x \neq 0$.

**Exemples**

- Montrons que les vecteurs 1 et $i$ sont linéairement indépendants dans le $\mathbb{R}$-espace vectoriel $\mathbb{C}$. Si $a$ et $b$ sont des nombres réels tels que $a + bi = 0$, alors $a = b = 0$. Cela signifie que 1 et $i$ sont linéairement indépendants. Par contre, si l'on considère $\mathbb{C}$ comme $\mathbb{C}$-espace vectoriel, alors 1 et $i$ ne sont pas linéairement indépendants : en effet, si l'on pose $\lambda = 1$ et $\mu = i$, alors $\lambda 1 + \mu i = 1 + i^2 = 0$.
- Soient $f$ et $g$ les éléments du $\mathbb{R}$-espace vectoriel des fonctions de $\mathbb{R}$ dans $\mathbb{R}$, définis par $f(x) = \cos x$ et $g(x) = \sin x$. Si $a$ et $b$ sont des nombres réels tels que $af + bg = 0$, il vient $a\cos x + b\sin x = 0$ pour tout $x \in \mathbb{R}$. En particulier, on a cette égalité si $x = 0$ et si $x = \pi/2$. On en déduit $a = 0$ et $b = 0$. Les vecteurs $f$ et $g$ sont donc linéairement indépendants.
- Considérons les matrices suivantes de $M_2(\mathbb{C})$ :

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} -1 & 0 \\ 0 & i \end{bmatrix} \quad \text{et} \quad C = \begin{bmatrix} i & 1 \\ 0 & 1 \end{bmatrix}.$$

Si $a, b, c$ sont des nombres complexes, nous avons les équivalences

$$aA + bB + cC = 0 \iff \begin{cases} a - b + ic = 0 \\ c = 0 \\ a + ib + c = 0 \end{cases} \iff \begin{cases} a - b = 0 \\ a + ib = 0 \\ c = 0 \end{cases}$$
$$\iff \begin{cases} a - b = 0 \\ (1+i)b = 0 \\ c = 0 \end{cases} \iff \begin{cases} a = 0 \\ b = 0 \\ c = 0. \end{cases}$$

On a ainsi démontré que si $a, b, c$ sont des nombres complexes tels que $aA + bB + cC = 0$, alors $a = b = c = 0$. Les vecteurs $A, B, C$ du $\mathbb{C}$-espace vectoriel $M_2(\mathbb{C})$ sont donc linéairement indépendants.





- Les vecteurs de $\mathbb{R}^3$ définis par $x_1 = (1,0,1)$, $x_2 = (0,1,0)$ et $x_3 = (1,1,1)$ ne sont pas linéairement indépendants : on a en effet $x_3 = x_1 + x_2$, donc $x_1 + x_2 + (-1)x_3 = 0$.

> Pour montrer que des vecteurs $x_1, x_2, \dots, x_n$ sont linéairement indépendants, il faut
> - se donner des lettres, par exemple $\lambda_1, \lambda_2, \dots, \lambda_n$, représentant des scalaires,
> - faire l'hypothèse que l'on a $\lambda_1 x_1 + \lambda_2 x_2 = \cdots + \lambda_n x_n = 0$,
> - puis démontrer que l'on a $\lambda_1 = \lambda_2 = \cdots = \lambda_n = 0$.

**Proposition.** *Soient $n$ un entier supérieur ou égal à 2 et $x_1, \dots, x_n$ des vecteurs de $E$ linéairement indépendants. Alors aucun des $x_i$ n'est le vecteur nul. De plus, les vecteurs $x_1, \dots, x_n$ sont deux à deux différents et pour tout entier positif $p$ tel que $p \leqslant n$, les vecteurs $x_1, \dots, x_p$ sont linéairement indépendants.*

**Démonstration.** Démontrons les deux premières propriétés, la troisième étant immédiate. Soit $i$ l'un des entiers compris entre 1 et $n$. Posons $\lambda_i = 1$ et $\lambda_j = 0$ pour tout entier $j \neq i$. Les vecteurs $x_1, \dots, x_n$ sont linéairement indépendants et les scalaires $\lambda_1, \dots, \lambda_n$ ne sont pas tous nuls, puisque $\lambda_i = 1$. On a donc $\lambda_1 x_1 + \cdots + \lambda_n x_n \neq 0$, c'est-à-dire $1x_i \neq 0$ ou encore $x_i \neq 0$. Soient $i, j$ deux entiers différents compris entre 1 et $n$. Posons $\mu_i = 1$, $\mu_j = -1$ et $\mu_k = 0$ pour tout entier $k \neq i, j$. Il vient $\mu_1 x_1 + \mu_2 x_2 + \cdots + \mu_n x_n \neq 0$, c'est-à-dire $x_i - x_j \neq 0$, ou encore $x_i \neq x_j$. ■

**Proposition.** *Soient $n$ un entier positif, $x_1, \dots, x_n$ des vecteurs de $E$ linéairement indépendants et $y$ un vecteur de $E$. Alors $y$ est combinaison linéaire de $x_1 \dots, x_n$ si et seulement si les vecteurs $x_1, \dots, x_n, y$ ne sont pas linéairement indépendants.*

**Démonstration.** S'il existe des scalaires $\lambda_1, \dots, \lambda_n$ tels que $y = \lambda_1 x_1 + \cdots + \lambda_n x_n$, il vient $\lambda_1 x_1 + \cdots + \lambda_n x_n - y = 0$, par suite les vecteurs $x_1, \dots, x_n, y$ ne sont pas linéairement indépendants.

Réciproquement, supposons que les vecteurs $x_1, \dots, x_n, y$ ne sont pas linéairement indépendants. Il existe donc des scalaires $\mu_1, \dots, \mu_n, \mu_{n+1}$ non tous nuls tels que $\mu_1 x_1 + \cdots + \mu_n x_n + \mu_{n+1} y = 0$. Si l'on avait $\mu_{n+1} = 0$, on aurait $\mu_1 x_1 + \cdots + \mu_n x_n = 0$ et donc $\mu_1 = \cdots = \mu_n = 0$, puisque les vecteurs $x_1 \dots, x_n$ sont linéairement indépendants. Les scalaires $\mu_i$ seraient tous nuls, ce qui est une contradiction. Par suite on a $\mu_{n+1} \neq 0$ et $y = -(\mu_1/\mu_{n+1})x_1 - \cdots - (\mu_n/\mu_{n+1})x_n$. Ainsi $y$ est combinaison linéaire de $x_1, \dots, x_n$. ■

Dans la proposition précédente, l'hypothèse que les vecteurs $x_1, \dots, x_n$ sont linéairement indépendants est cruciale : considérons par exemple les vecteurs de $\mathbb{R}^3$ définis

par $x_1=(1,0,0)$, $x_2=(0,1,0)$, $x_3=x_1+x_2$ et $y=(0,0,1)$ ; puisque $x_3$ est combinaison linéaire de $x_1$ et $x_2$, les vecteurs $x_1,x_2,x_3$ ne sont pas linéairement indépendants, donc $x_1,x_2,x_3,y$ non plus ; cependant le vecteur $y$ n'est pas combinaison linéaire des vecteurs $x_1,x_2,x_3$, car dans toute combinaison linéaire de $x_1,x_2,x_3$, la dernière coordonnée est nulle.

## 4. Bases et dimension

Dans ce paragraphe, $E$ est un espace vectoriel sur $\mathbf{K}$ et nous supposons que $E \neq \{0\}$, c'est-à-dire que $E$ contient des vecteurs autres que le vecteur nul.

**Définition**

Soient $n$ un entier positif et $e_1,\dots,e_n$ des vecteurs de $E$. On dit que $(e_1,\dots,e_n)$ est une *base* de $E$ si les vecteurs $e_1,\dots,e_n$ sont linéairement indépendants et si $E$ est engendré par les vecteurs $e_1,\dots,e_n$.

Lorsque $n=1$, on convient d'écrire que $e_1$ est une base de $E$.

**Exemples**

- Tout élément non nul de $\mathbf{K}$ est une base du $\mathbf{K}$-espace vectoriel $\mathbf{K}$. En effet, soit $a$ un élément non nul de $\mathbf{K}$. Pour tout $b \in \mathbf{K}$, on a $b=(b/a)a$, par suite $\mathbf{K}$ est engendré par $a$.
- Nous avons déjà remarqué que 1 et $i$ sont des vecteurs linéairement indépendants du $\mathbb{R}$-espace vectoriel $\mathbb{C}$. Puisque tout nombre complexe s'écrit $a+bi$ où $a$ et $b$ sont des nombres réels, $\mathbb{C}$ est engendré par 1 et $i$. Il s'ensuit que $(1,i)$ est une base du $\mathbb{R}$-espace vectoriel $\mathbb{C}$.
- Si $n$ est un entier supérieur ou égal à 2 et si $\mathbf{e}_1,\mathbf{e}_2,\dots,\mathbf{e}_n$ sont les vecteurs de $\mathbf{K}^n$ définis par

$$\mathbf{e}_1=(1,0,\dots,0),\quad \mathbf{e}_2=(0,1,\dots,0),\quad \dots\quad \mathbf{e}_n=(0,\dots,0,1),$$

alors $(\mathbf{e}_1,\mathbf{e}_2,\dots,\mathbf{e}_n)$ est une base de $\mathbf{K}^n$. Cette base s'appelle la *base canonique* de $\mathbf{K}^n$.
- Si $n$ est un entier supérieur ou égal à 2, rappelons que l'on a noté $E_1,E_2,\dots,E_n$ les matrices suivantes de $M_{n,1}(\mathbf{K})$ :

$$E_1=\begin{bmatrix}1\\0\\\vdots\\0\end{bmatrix},\quad E_2=\begin{bmatrix}0\\1\\\vdots\\0\end{bmatrix},\quad \dots\quad E_n=\begin{bmatrix}0\\\vdots\\0\\1\end{bmatrix}.$$





Alors $(E_1,E_2,\dots,E_n)$ est une base de $M_{n,1}(\mathbf{K})$ et $({}^tE_1,{}^tE_2,\dots,{}^tE_n)$ est une base de $M_{1,n}(\mathbf{K})$.
- Considérons les matrices suivantes de $M_2(\mathbf{K})$ :

$$E_{11}=\begin{bmatrix}1&0\\0&0\end{bmatrix},\quad E_{12}=\begin{bmatrix}0&1\\0&0\end{bmatrix},\quad E_{21}=\begin{bmatrix}0&0\\1&0\end{bmatrix},\quad E_{22}=\begin{bmatrix}0&0\\0&1\end{bmatrix}.$$

Alors $(E_{11},E_{12},E_{21},E_{22})$ est une base de $M_2(\mathbf{K})$.

Voici un théorème essentiel, tant sur le plan théorique que pratique.

**Théorème de la base incomplète.** *Soient $p$ un entier positif et $f_1,\dots,f_p$ des vecteurs de $E$ linéairement indépendants. Soient $q$ un entier positif et $g_1,\dots,g_q$ des vecteurs de $E$. On suppose que $E$ est engendré par $g_1,\dots,g_q$. Alors il existe un entier $n \geqslant p$ et une base $(e_1,\dots,e_n)$ de $E$, telle que*

$$e_i=f_i \text{ pour tout } i\leqslant p \text{ et } e_i \text{ est l'un des vecteurs } g_j \text{ pour tout } i>p.$$

**Démonstration**

*Premier cas* : supposons que pour tout entier $j$, le vecteur $g_j$ est combinaison linéaire des vecteurs $f_1,\dots,f_p$. Puisque tout vecteur de $E$ est combinaison linéaire des vecteurs $g_1,\dots,g_q$, il s'ensuit que tout vecteur de $E$ est combinaison linéaire des vecteurs $f_1,\dots,f_p$. Les vecteurs $f_1,\dots,f_p$ étant linéairement indépendants, $(f_1,\dots,f_p)$ est donc une base de $E$.

*Second cas* : supposons qu'il existe un entier $k$ tel que $g_k$ n'est pas combinaison linéaire des vecteurs $f_1,\dots,f_p$. D'après la dernière proposition du paragraphe précédent, les vecteurs $f_1,\dots,f_p,g_k$ sont linéairement indépendants. Considérons alors le plus grand entier $n$ compris entre $p+1$ et $p+q$ pour lequel il existe des vecteurs $e_1,\dots,e_n$ linéairement indépendants, tels que $e_i=f_i$ pour tout $i\leqslant p$ et $e_i$ est l'un des vecteurs $g_j$ pour tout $i>p$. Montrons que $(e_1,\dots,e_n)$ est une base de $E$. Puisque les vecteurs $e_1,\dots,e_n$ sont linéairement indépendants, il reste à démontrer que $E$ est engendré par $e_1,\dots,e_n$. Par définition de l'entier $n$, pour tout vecteur $g_j$, les vecteurs $e_1,\dots,e_n,g_j$ ne sont pas linéairement indépendants. Tout vecteur $g_j$ est donc combinaison linéaire des vecteurs $e_1,\dots,e_n$. Puisque tout vecteur de $E$ est combinaison linéaire des vecteurs $g_1,\dots,g_q$, il s'ensuit que tout vecteur de $E$ est combinaison linéaire des vecteurs $e_1,\dots,e_n$, ce qu'il fallait démontrer. ∎

**Théorème.** *Si $E$ est engendré par un nombre fini de vecteurs, alors il existe une base de $E$.*

**Démonstration.** Par hypothèse, il existe un entier $q\geqslant 1$ et des vecteurs $g_1,\dots,g_q$ tels que $E$ est engendré par $g_1,\dots,g_q$. Puisque $E\neq\{0\}$, il existe un vecteur $f\in E$, tel que $f\neq 0$. D'après le théorème de la base incomplète, où l'on choisit $p=1$, il existe une base $(e_1,\dots,e_n)$ de $E$ telle que $e_1=f$ et pour tout $i>p$, $e_i$ est l'un des vecteurs $g_j$. ∎

Ce théorème est important : il affirme en effet l'existence de base.

**Proposition.** *Supposons que $n$ est un entier positif et que $(e_1, \dots, e_n)$ est une base de $E$. Pour tout $x \in E$, il existe $x_1, \dots, x_n \in \mathbf{K}$ uniques tels que $x = x_1e_1 + \cdots + x_ne_n$. Les scalaires $x_1, \dots, x_n$ s'appellent les coordonnées de $x$ dans la base $(e_1, \dots, e_n)$.*

**Démonstration.** Soit $x \in E$. Les scalaires $x_1, \dots, x_n$ existent, puisque $E$ est engendré par les vecteurs $e_1, \dots, e_n$. De plus, si l'on a $x_1e_1 + \cdots + x_ne_n = y_1e_1 + \cdots + y_ne_n$, il vient $(x_1 - y_1)e_1 + \cdots + (x_n - y_n)e_n = 0$. Puisque les vecteurs $e_1, \dots, e_n$ sont linéairement indépendants, il s'ensuit $x_1 - y_1 = \cdots = x_n - y_n = 0$, c'est-à-dire $x_1 = y_1, \dots, x_n = y_n$. Les scalaires $x_1, \dots, x_n$ sont donc uniques. ∎

**Exemples**

- Considérons le $\mathbb{R}$-espace vectoriel $\mathbb{C}$. Si $a$ et $b$ sont des nombres réels, les coordonnées du nombre complexe $a + bi$ dans la base $(1, i)$ sont $a$ et $b$.
- Les coordonnées du vecteur $(x_1, x_2, \dots, x_n) \in \mathbf{K}^n$ dans la base canonique de $\mathbf{K}^n$ sont $x_1, x_2, \dots, x_n$.

**Remarque**

Supposons que $(e_1, \dots, e_n)$ est une base de $E$. Soient $x$ et $y$ des vecteurs de $E$. Notons $x_1, \dots, x_n$ les coordonnées de $x$ dans la base $(e_1, \dots, e_n)$ et notons $y_1, \dots, y_n$ celles de $y$. Alors les coordonnées du vecteur $x + y$ sont $x_1 + y_1, \dots, x_n + y_n$ et celles du vecteur $\lambda x$ sont $\lambda x_1, \dots, \lambda x_n$, si $\lambda$ est un scalaire.

**Exercice.** Soient les vecteurs $f_1 = (3, 5)$ et $f_2 = (4, 7)$ appartenant à $\mathbb{R}^2$. Montrer que $(f_1, f_2)$ est une base de l'espace vectoriel $\mathbb{R}^2$ et calculer les coordonnées du vecteur $(a, b) \in \mathbb{R}^2$ dans cette base.

**Réponse.** Montrons d'abord que les vecteurs $f_1, f_2$ engendrent l'espace vectoriel $\mathbb{R}^2$, c'est-à-dire que tout vecteur $(a, b) \in \mathbb{R}^2$ est combinaison linéaire de $f_1$ et $f_2$. Pour cela, cherchons des nombres $x_1$ et $x_2$ tels que $x_1f_1 + x_2f_2 = (a, b)$. Puisqu'on a

$$x_1f_1 + x_2f_2 = x_1(3,5) + x_2(4,7) = (3x_1 + 4x_2, 5x_1 + 7x_2),$$

l'égalité $x_1f_1 + x_2f_2 = (a, b)$ est équivalente aux systèmes

$$\begin{cases} 3x_1 + 4x_2 = a \\ 5x_1 + 7x_2 = b \end{cases} \Longleftrightarrow \begin{cases} 3x_1 + 4x_2 = a \\ x_2 = 3b - 5a \end{cases} \Longleftrightarrow \begin{cases} 3x_1 = a - 4(3b - 5a) \\ x_2 = 3b - 5a \end{cases} \Longleftrightarrow \begin{cases} x_1 = 7a - 4b \\ x_2 = 3b - 5a. \end{cases}$$

Ainsi nous avons l'égalité

$$(\bullet) \qquad (a, b) = (7a - 4b)f_1 + (3b - 5a)f_2.$$

Montrons maintenant que les vecteurs $f_1, f_2$ sont linéairement indépendants. Supposons que $x_1$ et $x_2$ sont des nombres réels tels que $x_1f_1 + x_2f_2 = 0$. Appliquons le calcul ci-dessus en choisissant $(a, b) = (0, 0)$ : il vient $x_1 = 0$ et $x_2 = 0$. Les vecteurs $f_1, f_2$ sont donc linéairement indépendants.

Ainsi $(f_1, f_2)$ est une base de l'espace vectoriel $\mathbb{R}^2$.

Les coordonnées du vecteur $(a, b)$ dans la base $(f_1, f_2)$ sont données par l'égalité $(\bullet)$ : ce sont les nombres $7a - 4b$, $3b - 5a$.





**Proposition.** *Supposons que $E$ possède une base formée de $n$ vecteurs. Si $p$ est un entier tel que $p > n$, alors $p$ vecteurs de $E$ ne sont pas linéairement indépendants.*

**Démonstration.** Soit $(e_1, \dots, e_n)$ une base de $E$. Supposons que $p$ est un entier tel que $p > n$ et que $f_1, f_2, \dots, f_p$ sont $p$ vecteurs de $E$. Pour tout $j \in \{1, 2, \dots, p\}$, notons $a_{1j}, \dots, a_{nj}$ les coordonnées de $f_j$ dans la base $(e_1, \dots, e_n)$, de sorte que l'on a

$$\begin{cases} f_1 = a_{11}e_1 + \cdots + a_{n1}e_n \\ f_2 = a_{12}e_1 + \cdots + a_{n2}e_n \\ \vdots \qquad\qquad \vdots \\ f_p = a_{1p}e_1 + \cdots + a_{np}e_n. \end{cases}$$

Pour tous $x_1, x_2, \dots, x_p \in \mathbf{K}$, le vecteur $x_1f_1 + x_2f_2 + \cdots + x_pf_p$ a pour coordonnées dans la base $(e_1, \dots, e_n)$ les scalaires

$$\begin{cases} y_1 = a_{11}x_1 + a_{12}x_2 + \cdots + a_{1p}x_p \\ \vdots \qquad\qquad \vdots \\ y_n = a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{np}y_p. \end{cases}$$

Puisqu'un vecteur est nul si et seulement si ses coordonnées dans la base $(e_1, \dots, e_n)$ sont nulles, on a l'équivalence

$$x_1f_1 + x_2f_2 + \cdots + x_pf_p = 0 \Longleftrightarrow \begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1p}x_p = 0 \\ \vdots \qquad\qquad \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{np}x_p = 0. \end{cases}$$

La matrice de ce système d'équations linéaires est la matrice $A = [a_{ij}]$ appartenant à $M_{n,p}(\mathbf{K})$. Puisqu'on a $p > n$, il existe une matrice-colonne $X \in M_{p,1}(\mathbf{K})$ telle que $X \neq 0$ et $AX = 0$, d'après le corollaire page 70. Autrement dit, il existe des scalaires $x_1, x_2, \dots, x_p$ non tous nuls tels que $x_1f_1 + x_2f_2 + \cdots + x_pf_p = 0$. Il s'ensuit que les vecteurs $f_1, f_2, \dots, f_p$ ne sont pas linéairement indépendants. ∎

**Théorème.** *Si $E$ est engendré par un nombre fini de vecteurs, alors toutes les bases de $E$ ont le même nombre de vecteurs.*

**Démonstration.** Soient $(e_1, \dots, e_n)$ et $(f_1, \dots, f_p)$ deux bases de $E$. Puisque les $p$ vecteurs $f_1, \dots, f_p$ sont linéairement indépendants, on a $p \leqslant n$, d'après la proposition précédente. Puisque $e_1, \dots, e_n$ sont linéairement indépendants, on a de même $n \leqslant p$. Il s'ensuit $n = p$. ∎

**Définition**
Supposons $E$ engendré par un nombre fini de vecteurs. Le nombre de vecteurs qui forment une base de $E$ s'appelle la *dimension* de $E$ et se note $\dim E$. De plus, on définit la dimension de l'espace vectoriel $\{0\}$ en posant $\dim\{0\} = 0$.

Dorénavant, au lieu d'écrire que $E$ est engendré par un nombre fini de vecteurs, nous écrirons que $E$ est de *dimension finie*.

**Exemples**

- Le $\mathbf{R}$-espace vectoriel $\mathbf{C}$ est de dimension 2, car $(1, i)$ est une base de $\mathbf{C}$.
- Soit $n$ un entier supérieur ou égal à 2. Alors $\mathbf{K}^n$ est un $\mathbf{K}$-espace vectoriel de dimension $n$, puisque la base canonique de $\mathbf{K}^n$ est formée de $n$ vecteurs.
- Le $\mathbf{K}$-espace vectoriel $M_2(\mathbf{K})$ est de dimension 4, car une base de $M_2(\mathbf{K})$ est formée des matrices

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \quad \text{et} \quad \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

- Plus généralement, l'espace vectoriel $M_{n,p}(\mathbf{K})$ est de dimension $np$. En effet, notons $E_{ij}$ la matrice de $M_{n,p}(\mathbf{K})$ dont le coefficient à l'intersection de la ligne $i$ et de la colonne $j$ est égal à 1 et dont tous les autres coefficients sont nuls. Alors les vecteurs $E_{ij}$ forment une base de $M_{n,p}(\mathbf{K})$. En particulier la dimension de $M_n(\mathbf{K})$ est égale à $n^2$.

**Définitions**
Un espace vectoriel de dimension 1 s'appelle une *droite vectorielle* ou plus simplement une *droite* et un espace vectoriel de dimension 2 s'appelle un *plan vectoriel* ou plus simplement un *plan*.

**Proposition.** *Si $F$ et $G$ sont des $\mathbf{K}$-espaces vectoriels de dimension finie, alors l'espace vectoriel $F \times G$ est de dimension finie et l'on a* $\dim(F \times G) = \dim F + \dim G$.

**Démonstration.** Démontrons ce résultat lorsque $F \neq \{0\}$ et $G \neq \{0\}$. Soient $(f_1, \dots, f_p)$ une base de $F$ et $(g_1, \dots, g_q)$ une base de $G$. Considérons les $p+q$ vecteurs suivants de $F \times G$ : $e_i = (f_i, 0)$ pour tout $i \in \{1, \dots, p\}$ et $e_{p+j} = (0, g_j)$ pour tout $j \in \{1, \dots, q\}$. Soit $x$ un vecteur de $F \times G$. Par définition du produit, il existe $y \in F$ et $z \in G$ tels que $x = (y, z)$, c'est-à-dire $x = (y, 0) + (0, z)$. Puisque $y$ est combinaison linéaire de $f_1, \dots, f_p$ et puisque $z$ est combinaison linéaire de $g_1, \dots, g_q$, il s'ensuit que $x$ est combinaison linéaire des vecteurs $e_1, \dots, e_{p+q}$. D'autre part, si $x_1, \dots, x_{p+q}$ sont des scalaires tels que $x_1 e_1 + \dots + x_{p+q} e_{p+q} = 0$, c'est-à-dire tels que

$$(x_1 f_1 + \dots + x_p f_p, x_{p+1} g_1 + \dots + x_{p+q} g_q) = (0, 0),$$



il vient $x_1 f_1 + \dots + x_p f_p = 0$ et $x_{p+1} g_1 + \dots + x_{p+q} g_q = 0$. On en déduit $x_1 = \dots = x_p = 0$ et $x_{p+1} = \dots = x_{p+q} = 0$. Les vecteurs $e_1, \dots, e_{p+q}$ sont donc linéairement indépendants. Par conséquent $(e_1, \dots, e_{p+q})$ est une base de $F \times G$. ∎

Les deux énoncés qui suivent sont utiles lorsqu'on veut démontrer que des vecteurs d'un espace vectoriel de dimension $n$ forment une base.

**Théorème.** *Supposons $E$ de dimension $n$.*

- *Si $p$ vecteurs de $E$ sont linéairement indépendants, alors $p \leqslant n$. De plus, si $n$ vecteurs de $E$ sont linéairement indépendants, alors ils forment une base de $E$.*
- *Si $E$ est engendré par $q$ vecteurs, alors $q \geqslant n$. De plus, si $n$ vecteurs de $E$ engendrent $E$, alors ils forment une base de $E$.*

**Démonstration.** Supposons que $f_1, \dots, f_p$ sont $p$ vecteurs de $E$ linéairement indépendants. D'après une proposition page 113, on a $p \leqslant n$. Supposons $p = n$ et montrons que $E$ est engendré par $f_1, \dots, f_n$. Si $x$ est un vecteur différent de tous les $f_i$, alors d'après ce qui précède, les $n+1$ vecteurs $f_1, \dots, f_n, x$ ne sont pas linéairement indépendants, par suite $x$ est combinaison linéaire de $f_1, \dots, f_n$. Tout vecteur de $E$ est combinaison linéaire des vecteurs $f_1, \dots, f_n$, donc $(f_1, \dots, f_n)$ est une base de $E$. Supposons que $E$ est engendré par les $q$ vecteurs $g_1, \dots, g_q$. Puisque $E$ contient d'autres vecteurs que le vecteur nul et puisque tout vecteur de $E$ est combinaison linéaire de $g_1, \dots, g_q$, l'un des vecteurs $g_j$ n'est pas nul. D'après le théorème de la base incomplète, on peut compléter ce vecteur de manière à obtenir une base de $E$ formée de $n$ vecteurs pris parmi $g_1, \dots, g_q$. Il s'ensuit $n \leqslant q$. De plus, si l'on a $q = n$, alors cette base est nécessairement formée de tous les vecteurs $g_1, \dots, g_n$. ∎

**Corollaire.** *Supposons $E$ de dimension $n \geqslant 1$. Soient $(e_1, \dots, e_n)$ une base de $E$ et $f_1, \dots, f_n$ des vecteurs de $E$. Notons $A$ la matrice de $M_n(\mathbf{K})$ dont les coefficients de la $j$-ième colonne sont les coordonnées du vecteur $f_j$ dans la base $(e_1, \dots, e_n)$. Alors $(f_1, \dots, f_n)$ est une base de $E$ si et seulement si la matrice $A$ est inversible.*

**Démonstration.** Posons $A = [a_{ij}]$, de sorte que l'on a

$$\begin{cases} f_1 = a_{11} e_1 + \dots + a_{n1} e_n \\ f_2 = a_{12} e_1 + \dots + a_{n2} e_n \\ \vdots \qquad\qquad \vdots \\ f_n = a_{1n} e_1 + \dots + a_{nn} e_n. \end{cases}$$

Pour tous $x_1, x_2, \ldots, x_n \in \mathbf{K}$, le vecteur $x_1 f_1 + x_2 f_2 + \cdots + x_n f_n$ a pour coordonnées dans la base $(e_1, \ldots, e_n)$ les scalaires

$$\begin{cases} y_1 = a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ \vdots \qquad\qquad \vdots \\ y_n = a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}y_n. \end{cases}$$

Puisqu'un vecteur est nul si et seulement si ses coordonnées dans la base $(e_1, \ldots, e_n)$ sont nulles, on a l'équivalence

$$x_1 f_1 + x_2 f_2 + \cdots + x_n f_n = 0 \Longleftrightarrow \begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0 \\ \vdots \qquad\qquad \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n = 0. \end{cases}$$

Or la matrice de ce système d'équations linéaires est $A$. Ce système a pour seule solution $x_1 = x_2 = \cdots = x_n = 0$ si et seulement si la matrice $A$ est inversible. Il s'ensuit que les vecteurs $f_1, f_2, \ldots, f_n$ sont linéairement indépendants si et seulement si la matrice $A$ est inversible. On conclut grâce au théorème précédent. ∎

**Exemple.** Soit $m$ un nombre réel. On considère les vecteurs de $\mathbf{R}^4$ : $f_1 = (1, m, 1, 0)$, $f_2 = (1, 0, 0, 1)$, $f_3 = (1, 1, m, 1)$ et $f_4 = (1, 1, 1, 1)$. Choisissons comme base de $\mathbf{R}^4$ la base canonique $(\mathrm{e}_1, \mathrm{e}_2, \mathrm{e}_3, \mathrm{e}_4)$. Rappelons que $\mathrm{e}_1 = (1, 0, 0, 0)$, $\mathrm{e}_2 = (0, 1, 0, 0)$, $\mathrm{e}_3 = (0, 0, 1, 0)$ et $\mathrm{e}_4 = (0, 0, 0, 1)$. D'après le corollaire ci-dessus, $(f_1, f_2, f_3, f_4)$ est une base de $\mathbf{R}^4$ si et seulement si la matrice

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 \\ m & 0 & 1 & 1 \\ 1 & 0 & m & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

est inversible, donc si et seulement si $\det A \neq 0$. Pour calculer $\det A$, retranchons la dernière ligne à la première, puis développons selon la première ligne. Il vient

$$\det A = \begin{vmatrix} 1 & 1 & 1 & 1 \\ m & 0 & 1 & 1 \\ 1 & 0 & m & 1 \\ 0 & 1 & 1 & 1 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 & 0 \\ m & 0 & 1 & 1 \\ 1 & 0 & m & 1 \\ 0 & 1 & 1 & 1 \end{vmatrix} = \begin{vmatrix} 0 & 1 & 1 \\ 0 & m & 1 \\ 1 & 1 & 1 \end{vmatrix} = \begin{vmatrix} 1 & 1 \\ m & 1 \end{vmatrix} = 1 - m.$$

Il s'ensuit que $(f_1, f_2, f_3, f_4)$ est une base de $\mathbf{R}^4$ si et seulement si $m \neq 1$.

### Changement de coordonnées

Considérons les vecteurs de $\mathbf{R}^4$ : $f_1 = (1, 0, 1, 0)$, $f_2 = (1, 0, 0, 1)$, $f_3 = (1, 1, 0, 1)$ et $f_4 = (1, 1, 1, 1)$. D'après l'exemple ci-dessus (avec $m=0$), $(f_1, f_2, f_3, f_4)$ est une base de $\mathbf{R}^4$. Soit $u$ le vecteur de $\mathbf{R}^4$ dont les coordonnées dans la base canonique sont $a, b, c, d$, autrement dit $u = (a, b, c, d)$. Cherchons les coordonnées de $u$ dans la base $(f_1, f_2, f_3, f_4)$, c'est-à-dire





cherchons les nombres réels $x, y, z, t$ tels que $(a, b, c, d) = x f_1 + y f_2 + z f_3 + t f_4$. Or on a

$$\begin{aligned} x f_1 + y f_2 + z f_3 + t f_4 &= x(1, 0, 1, 0) + y(1, 0, 0, 1) + z(1, 1, 0, 1) + t(1, 1, 1, 1) \\ &= (x + y + z + t, z + t, x + t, y + z + t), \end{aligned}$$

et les systèmes équivalents suivants :

$$\begin{cases} x + y + z + t = a \\ y + z + t = d \\ x + t = c \\ z + t = b \end{cases} \Longleftrightarrow \begin{cases} x = a - d \\ y + z + t = d \\ t = c - a + d \\ z + t = b \end{cases} \Longleftrightarrow \begin{cases} x = a - d \\ t = -a + c + d \\ z = a + b - c - d \\ y = -b + d. \end{cases}$$

On a donc $(a, b, c, d) = (a - d)f_1 + (-b + d)f_2 + (a + b - c - d)f_3 + (-a + c + d)f_4$. En particulier, nous obtenons les coordonnées des vecteurs de la base canonique de $\mathbf{R}^4$ dans la base $(f_1, f_2, f_3, f_4)$. Il vient

$$\begin{cases} \mathrm{e}_1 = f_1 + f_3 - f_4 \\ \mathrm{e}_2 = -f_2 + f_3 \\ \mathrm{e}_3 = -f_3 + f_4 \\ \mathrm{e}_4 = -f_1 + f_2 - f_3 + f_4. \end{cases}$$

**Exercice 1.** Soit $a$ un nombre réel. On considère les vecteurs de $\mathbf{R}^3$ : $f_1 = (2, a, 0)$ et $f_2 = (0, -1, a + 1)$.

a) Montrer que les vecteurs $f_1$ et $f_2$ sont linéairement indépendants.

b) Compléter les vecteurs $f_1$ et $f_2$ pour former une base de $\mathbf{R}^3$.

**Réponse.** Notons $(\mathrm{e}_1, \mathrm{e}_2, \mathrm{e}_3)$ la base canonique de $\mathbf{R}^3$.

a) La deuxième coordonnée de $f_2$ dans la base $(\mathrm{e}_1, \mathrm{e}_2, \mathrm{e}_3)$ est égal à $-1$, par suite $f_2$ n'est pas le vecteur nul. D'autre part, la première coordonnée de $f_2$ est nulle alors que celle de $f_1$ est égal à 2, donc $f_1$ n'est pas colinéaire à $f_2$. Il s'ensuit que les vecteurs $f_1$ et $f_2$ sont linéairement indépendants.

b) Une base de $\mathbf{R}^3$ est formée de trois vecteurs. Puisque $f_1, f_2$ sont linéairement indépendants, le théorème de la base incomplète affirme qu'il existe $i \in \{1, 2, 3\}$ tel que $(f_1, f_2, \mathrm{e}_i)$ est une base de $\mathbf{R}^3$. Dans la pratique, voici les résultats.
Si $a = 0$, alors $(f_1, f_2, \mathrm{e}_2)$ et $(f_1, f_2, \mathrm{e}_3)$ sont des bases de $\mathbf{R}^3$, alors que $(f_1, f_2, \mathrm{e}_1)$ n'en est pas une puisque $\mathrm{e}_1$ est colinéaire à $f_1$.
Si $a = -1$, alors $(f_1, f_2, \mathrm{e}_3)$ est une base de $\mathbf{R}^3$, alors que ni $(f_1, f_2, \mathrm{e}_1)$ ni $(f_1, f_2, \mathrm{e}_2)$ n'en sont puisque $\mathrm{e}_2$ est colinéaire à $f_2$ et $\mathrm{e}_1$ est colinéaire à $f_1 - f_2$.
Si $a \neq 0$ et $a \neq -1$, alors $(f_1, f_2, \mathrm{e}_i)$ est une base de $\mathbf{R}^3$ pour tout $i = 1, 2$ ou $3$. Si $a \neq 0$ et $a \neq -1$, alors $(f_1, f_2, \mathrm{e}_i)$ est une base de $\mathbf{R}^3$ (les Démontrons par exemple que si $a \neq -1$, alors $(f_1, f_2, \mathrm{e}_2)$ est une base de $\mathbf{R}^3$ (les autres cas se traitent de la même manière). Le déterminant de la matrice dont les colonnes sont les coordonnées des vecteurs $f_1$, $f_2$ et $\mathrm{e}_2$ dans la base $(\mathrm{e}_1, \mathrm{e}_2, \mathrm{e}_3)$ est

$$\begin{vmatrix} 2 & 0 & 0 \\ a & -1 & 1 \\ 0 & a + 1 & 0 \end{vmatrix} = 2 \begin{vmatrix} -1 & 1 \\ a + 1 & 0 \end{vmatrix} = -2(a + 1).$$

Puisque ce déterminant est non nul, on en déduit que $(f_1, f_2, \mathrm{e}_2)$ est une base de $\mathbf{R}^3$.

**Exercice 2.** Considérons les vecteurs de $\mathbb{R}^4$ : $f_1 = (1, 1, -1, 2)$, $f_2 = (0, 1, 2, 3)$ et $f_3 = (1, 0, 1, 0)$.

a) Montrer que les vecteurs $f_1$, $f_2$ et $f_3$ sont linéairement indépendants.

b) Soit $F$ le sous-espace vectoriel de $\mathbb{R}^4$ engendré par $f_1$, $f_2$ et $f_3$. Montrer que le vecteur $(x, y, z, t)$ de $\mathbb{R}^4$ appartient à $F$ si et seulement si $2x - 10y - z + 4t = 0$.

**Réponse**

a) Notons $\mathbf{e}_1$ le premier vecteur de la base canonique de $\mathbb{R}^4$ et $A$ la matrice dont les colonnes sont les coordonnées des vecteurs $f_1, f_2, f_3, \mathbf{e}_1$ dans la base canonique de $\mathbb{R}^4$. En utilisant les règles de calcul d'un déterminant, on obtient

$$\det A = \begin{vmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ -1 & 2 & 1 & 0 \\ 2 & 3 & 0 & 0 \end{vmatrix} = -\begin{vmatrix} 1 & 1 & 0 \\ -1 & 2 & 1 \\ 2 & 3 & 0 \end{vmatrix} = \begin{vmatrix} 1 & 1 \\ 2 & 3 \end{vmatrix} = 1.$$

Puisque $\det A \neq 0$, il s'ensuit que $(f_1, f_2, f_3, \mathbf{e}_1)$ est une base de $\mathbb{R}^4$. En particulier, les vecteurs $f_1, f_2, f_3, \mathbf{e}_1$ sont linéairement indépendants, donc les vecteurs $f_1, f_2, f_3$ sont a *fortiori* linéairement indépendants.

b) Soit $u=(x,y,z,t)$ un vecteur de $\mathbb{R}^4$. Le vecteur $u$ appartient à $F$ si et seulement si $u$ est combinaison linéaire de $f_1, f_2, f_3$, donc si et seulement si les vecteurs $f_1, f_2, f_3, u$ ne sont pas linéairement indépendants, puisque les vecteurs $f_1, f_2, f_3$ le sont. Or les vecteurs $f_1, f_2, f_3, u$ ne sont pas linéairement indépendants si et seulement si $(f_1, f_2, f_3, u)$ n'est pas une base de $\mathbb{R}^4$. On en déduit que $u$ appartient à $F$ si et seulement si on a

$$\begin{vmatrix} 1 & 0 & 1 & x \\ 1 & 1 & 0 & y \\ -1 & 2 & 1 & z \\ 2 & 3 & 0 & t \end{vmatrix} = 0.$$

Développons ce déterminant selon la dernière colonne :

$$\begin{vmatrix} 1 & 0 & 1 & x \\ 1 & 1 & 0 & y \\ -1 & 2 & 1 & z \\ 2 & 3 & 0 & t \end{vmatrix} = -x\begin{vmatrix} 1 & 1 & 0 \\ -1 & 2 & 1 \\ 2 & 3 & 0 \end{vmatrix} + y\begin{vmatrix} 1 & 0 & 1 \\ -1 & 2 & 1 \\ 2 & 3 & 0 \end{vmatrix} - z\begin{vmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 2 & 3 & 0 \end{vmatrix} + t\begin{vmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ -1 & 2 & 1 \end{vmatrix}.$$

D'après les règles de calcul d'un déterminant, il vient

$$\begin{vmatrix} 1 & 1 & 0 \\ -1 & 2 & 1 \\ 2 & 3 & 0 \end{vmatrix} = -\begin{vmatrix} 1 & 1 \\ 2 & 3 \end{vmatrix} = -1, \quad \begin{vmatrix} 1 & 0 & 1 \\ -1 & 2 & 1 \\ 2 & 3 & 0 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 \\ -1 & 2 & 2 \\ 2 & 3 & -2 \end{vmatrix} = \begin{vmatrix} 2 & 2 \\ 3 & -2 \end{vmatrix} = -10,$$

$$\begin{vmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 2 & 3 & 0 \end{vmatrix} = \begin{vmatrix} 1 & 1 \\ 2 & 3 \end{vmatrix} = 1 \quad \text{et} \quad \begin{vmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ -1 & 2 & 1 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 \\ 1 & 1 & -1 \\ -1 & 2 & 2 \end{vmatrix} = \begin{vmatrix} 1 & -1 \\ 2 & 2 \end{vmatrix} = 4.$$

Le vecteur $u$ appartient donc à $F$ si et seulement si $x - 10y - z + 4t = 0$.

Dans l'exercice précédent, la méthode utilisée pour démontrer que les vecteurs $f_1, f_2, f_3$ sont linéairement indépendants est justifiée par le théorème de la base incomplète. Ce théorème affirme en effet que l'on peut compléter trois vecteurs linéairement indépendants de $\mathbb{R}^4$ par un vecteur de la base canonique pour former une base de $\mathbb{R}^4$.





## Sous-espaces vectoriels en dimension finie

Supposons $E$ de dimension finie. Si $(e_1, \ldots, e_n)$ est une base de $E$ et si $F$ est un sous-espace vectoriel de $E$, alors tout vecteur de $F$ est combinaison linéaire de $e_1, \ldots, e_n$. En général, les vecteurs $e_i$ n'appartiennent pas à $F$. Nous allons montrer néanmoins que $F$ est engendré par un nombre fini de vecteurs.

**Théorème.** *Supposons $E$ de dimension $n$. Si $F$ est un sous-espace vectoriel de $E$, alors $F$ est de dimension finie, inférieure ou égale à $n$. De plus, si $\dim F = n$ alors $F = E$.*

**Démonstration.** Si $F = \{0\}$ alors $\dim F = 0$. Supposons $F \neq \{0\}$, c'est-à-dire qu'il existe un vecteur non nul appartenant à $F$. D'après une proposition précédente (page 113), $n+1$ vecteurs de $E$ ne sont pas linéairement indépendants. En particulier $n+1$ vecteurs de $F$ ne sont pas linéairement indépendants. Il existe donc un plus grand entier $p$ compris entre 1 et $n$ pour lequel on peut trouver $p$ vecteurs de $F$ linéairement indépendants, disons $f_1, \ldots, f_p$. Soit $x$ un vecteur de $F$, différent de tous les vecteurs $f_i$. Les $p+1$ vecteurs $f_1, \ldots, f_p, x$ ne sont pas linéairement indépendants. Puisque les vecteurs $f_1, \ldots, f_p$ le sont, $x$ est combinaison linéaire de $f_1, \ldots, f_p$. Il s'ensuit que $F$ est engendré par $f_1, \ldots, f_p$ et donc que $(f_1, \ldots, f_p)$ est une base de $F$. Le sous-espace vectoriel $F$ est donc de dimension $p$ et l'on a $p \leqslant n$. Si $p = n$, alors les vecteurs $f_1, \ldots, f_n$ sont linéairement indépendants, donc forment une base de $E$ (voir le théorème précédent page 115). Ainsi $F$ contient une base de $E$, donc aussi toute combinaison linéaire des vecteurs de cette base, par suite $F = E$. ■

**Proposition.** *Si $E$ est de dimension finie et si $F$ est un sous-espace vectoriel de $E$ de dimension $p \geqslant 1$, alors il existe une base de $E$ dont les $p$ premiers vecteurs appartiennent à $F$.*

**Démonstration.** Posons $n = \dim E$. Si $p = n$, alors on a $F = E$ et le résultat est vrai. Supposons $p < n$ et notons $(e_1, \ldots, e_p)$ une base de $F$. Puisque les vecteurs $e_1, \ldots, e_p$ sont linéairement indépendants, le théorème de la base incomplète affirme que l'on peut les compléter par $n - p$ vecteurs choisis dans une base de $E$, pour former une base de $E$. ■

**Proposition.** *Supposons $E$ de dimension finie. Soient $F$ et $G$ des sous-espaces vectoriels de $E$ différents de $\{0\}$. Si $(e_1, \ldots, e_p)$ est une base de $F$ et si $(e_{p+1}, \ldots, e_{p+q})$ est une base de $G$, alors les sous-espaces vectoriels $F$ et $G$ sont supplémentaires si et seulement si $(e_1, \ldots, e_{p+q})$ est une base de $E$.*

**Démonstration.** Supposons que $F$ et $G$ sont supplémentaires, c'est-à-dire que l'on a $F + G = E$ et $F \cap G = \{0\}$. Soit $z \in E$. Il existe $x \in F$ et $y \in G$ tels que $z = x + y$, donc $z$ est combinaison linéaire des vecteurs $e_1, \ldots, e_{p+q}$. D'autre part, si $x_1, \ldots, x_{p+q}$ sont des scalaires tels que $x_1 e_1 + \cdots + x_{p+q} e_{p+q} = 0$, il vient $x_1 e_1 + \cdots + x_p e_p = -x_{p+1} e_{p+1} - \cdots - x_{p+q} e_{p+q}$ et ainsi $x_1 e_1 + \cdots + x_p e_p \in F \cap G$. Puisque

$F \cap G = \{0\}$, on en déduit $x_1 e_1 + \cdots + x_p e_p = 0$. Les vecteurs $e_1, \ldots, e_p$ étant linéairement indépendants, il vient $x_1 = \cdots = x_p = 0$. De même on a $x_{p+1} = \cdots = x_{p+q} = 0$, car les vecteurs $e_{p+1}, \ldots, e_{p+q}$ sont linéairement indépendants. Les vecteurs $e_1, \ldots, e_{p+q}$ sont donc linéairement indépendants et par suite $(e_1, \ldots, e_{p+q})$ est une base de $E$.

Réciproquement, supposons que $(e_1, \ldots, e_{p+q})$ est une base de $E$. Chaque vecteur $e_i$ appartient à $F$ ou à $G$, donc à $F+G$. Il s'ensuit que $F+G$ contient une base de $E$, par suite $F+G=E$. D'autre part, soit $x \in F \cap G$. Puisque $(e_1, \ldots, e_p)$ est une base de $F$ et puisque $(e_{p+1}, \ldots, e_{p+q})$ est une base de $G$, il existe des scalaires $x_1, \ldots, x_{p+q}$ tels que $x = x_1 e_1 + \cdots + x_p e_p$ et $x = x_{p+1} e_{p+1} + \cdots + x_{p+q} e_{p+q}$. Il vient $x_1 e_1 + \cdots + x_p e_p - x_{p+1} e_{p+1} - \cdots - x_{p+q} e_{p+q} = 0$. Les vecteurs $e_1, \ldots, e_{p+q}$ étant linéairement indépendants, on en déduit $x_1 = \cdots = x_{p+q} = 0$, donc $x = 0$. Le seul élément de $F \cap G$ est donc le vecteur nul. On a $F+G=E$ et $F \cap G = \{0\}$, par suite $F$ et $G$ sont supplémentaires. ∎

Dans la proposition précédente, si $F$ et $G$ sont supplémentaires, alors $\dim E = \dim F + \dim G$. Cette égalité est encore vraie si l'un des sous-espaces vectoriels $F$ ou $G$ est $\{0\}$.

> Si $E$ est de dimension finie et si $E = F \oplus G$, alors on a $\dim E = \dim F + \dim G$.

**Corollaire.** *Si $E$ est de dimension finie, alors tout sous-espace vectoriel de $E$ a un supplémentaire.*

**Démonstration.** Soit $F$ un sous-espace vectoriel de $E$. Puisque $\{0\}$ et $E$ sont des sous-espaces vectoriels de $E$ supplémentaires, on peut supposer que $F$ est différent de $\{0\}$ et de $E$. Posons $n = \dim E$ et $p = \dim F$ ; on a donc $1 \leqslant p < n$. Nous savons qu'il existe une base $(e_1, \ldots, e_n)$ de $E$ telle que $(e_1, \ldots, e_p)$ est une base de $F$. Notons $G$ le sous-espace vectoriel de $E$ engendré par les vecteurs $e_{p+1}, \ldots, e_n$. Puisque les vecteurs $e_{p+1}, \ldots, e_n$ sont linéairement indépendants, $(e_{p+1}, \ldots, e_n)$ est une base de $G$. D'après la proposition précédente, on a $E = F \oplus G$. ∎

Terminons ce paragraphe en donnant la dimension de la somme de deux sous-espaces vectoriels.

**Proposition.** *Supposons $E$ de dimension finie. Si $F$ et $G$ sont des sous-espaces vectoriels de $E$, alors on a $\dim(F+G) = \dim F + \dim G - \dim(F \cap G)$.*

**Démonstration.** Puisque $F \cap G$ est un sous-espace vectoriel de $G$ et puisque $G$ est de dimension finie, il existe un sous-espace vectoriel de $G$ noté $G'$, tel que





$G = (F \cap G) \oplus G'$. On a $(F \cap G) + G' = G$ et $(F \cap G) \cap G' = \{0\}$. Puisque $G' \subset G$, $G'$ est un sous-espace vectoriel de $F+G$. Montrons que $F$ et $G'$ sont des sous-espaces vectoriels supplémentaires de $F+G$.

Soit $z \in F+G$. On a $z = x + y$ où $x \in F$ et $y \in G$. Il existe $y_1 \in F \cap G$ et $y_2 \in G'$ tels que $y = y_1 + y_2$ et par suite on a $z = (x + y_1) + y_2$. Puisque les vecteurs $x$ et $y_1$ appartiennent à $F$, on a $x + y_1 \in F$. Tout vecteur de $F+G$ est donc la somme d'un vecteur de $F$ et d'un vecteur de $G'$, autrement dit on a $F+G = F+G'$.

Soit $z \in F \cap G'$. Puisque $G' \subset G$, on a $z \in G$, donc $z \in F \cap G$ et par suite $z$ appartient à $F \cap G$ et à $G'$. Or on a $(F \cap G) \cap G' = \{0\}$, donc $z = 0$. Ainsi on a $F \cap G' = \{0\}$.

Puisque $F$ et $G'$ sont des sous-espaces vectoriels supplémentaires de $F+G$, on a $\dim F + \dim G' = \dim(F+G)$. Puisque $F \cap G$ et $G'$ sont des sous-espaces vectoriels supplémentaires de $G$, on a $\dim(F \cap G) + \dim G' = \dim G$. En retranchant ces deux égalités, on obtient $\dim F - \dim(F \cap G) = \dim(F+G) - \dim G$, d'où le résultat. ∎

## 5. Sous-espaces vectoriels de $\mathbb{K}^n$

Dans ce paragraphe, $n$ est un entier supérieur ou égal à 2.

Il y a deux façons de décrire un sous-espace vectoriel $F$ de $\mathbb{K}^n$ : ou bien se donner des équations de $F$, autrement dit considérer $F$ comme l'ensemble des vecteurs $(x_1, x_2, \ldots, x_n)$ de $\mathbb{K}^n$ solutions d'un système d'équations linéaires, ou bien se donner une base de $F$, ce qui permet de paramétrer $F$, c'est-à-dire de trouver explicitement tous les vecteurs de $F$. Chaque description a son utilité. Lorsqu'on a des équations de $F$, on teste aisément si un vecteur donné de $\mathbb{K}^n$ appartient ou non à $F$. Lorsqu'on connaît une base de $F$, on trouve rapidement des vecteurs appartenant effectivement à $F$.

Il est indispensable de savoir passer d'une description à l'autre. Lorsqu'on a affaire à un sous-espace vectoriel engendré par un nombre fini de vecteurs, on commencera par en chercher une base.

### Passage d'équations à base

Pour cela, on résout un système d'équations linéaires. Si la matrice $A$ de ce système n'est pas en échelons, on commence par pratiquer la méthode de Gauss comme au chapitre 4 paragraphe 4, pour se ramener à un système dont la matrice est en échelons. Dans le cas d'une matrice en échelons, présentons sur un exemple la méthode employée pour trouver une base de $F$.

**Exemple.** Soit $F$ le sous-espace vectoriel de $\mathbb{R}^4$ constitué des vecteurs $(x, y, z, t)$ tels que $\begin{cases} x + y - z + t = 0 \\ z - 2t = 0 \end{cases}$. La matrice de ce système est $\begin{bmatrix} 1 & 1 & -1 & 1 \\ 0 & 0 & 1 & -2 \end{bmatrix}$ ; elle est en échelons. La première équation commence par $x$ et la deuxième par $z$ : on écrit

alors $x$ et $z$ en fonction des autres coordonnées du vecteur $(x, y, z, t)$ dans la base canonique de $\mathbb{R}^4$, c'est-à-dire ici en fonction de $y$ et $t$. Précisément, on a

$$\begin{cases} x + y - z + t = 0 \\ z - 2t = 0 \end{cases} \iff \begin{cases} x = -y + t \\ z = 2t. \end{cases}$$

Traduisons ces égalités en une égalité de vecteurs de $\mathbb{R}^4$. Il vient

$$\begin{cases} x + y - z + t = 0 \\ z - 2t = 0 \end{cases} \iff (x, y, z, t) = (-y + t, y, 2t, t)$$
$$\iff (x, y, z, t) = y(-1, 1, 0, 0) + t(1, 0, 2, 1).$$

Posons $f_1 = (-1, 1, 0, 0)$ et $f_2 = (1, 0, 2, 1)$. D'après les équivalences ci-dessus, les vecteurs $f_1$ et $f_2$ appartiennent à $F$ et tout vecteur de $F$ est combinaison linéaire de $f_1$ et $f_2$, donc les vecteurs $f_1$ et $f_2$ engendrent $F$. D'autre part, on a

$$yf_1 + tf_2 = 0 \iff (-y + t, y, 2t, t) = 0 \iff y = t = 0$$

donc les vecteurs $f_1$ et $f_2$ sont linéairement indépendants. Il s'ensuit que $(f_1, f_2)$ est une base de $F$.

De manière générale, une fois la méthode de Gauss pratiquée, la dimension de $F$ est égale à $n - r$, où $r$ est le nombre d'équations effectivement écrites. De plus, une base de $F$ est obtenue en écrivant la coordonnée qui figure en tête de chaque équation en fonction de toutes celles qui ne sont pas écrites en tête.

**Exercice.** Considérons les sous-espaces vectoriels de $\mathbb{R}^4$ :

$$F = \{ (x, y, z, t) \in \mathbb{R}^4 \mid x - y - 2t = 0 \text{ et } x + t = 0 \}$$
$$G = \{ (x, y, z, t) \in \mathbb{R}^4 \mid x - z + t = 0 \text{ et } y + z = 0 \}.$$

a) Trouver une base de $F$ et une base de $G$.

b) Les sous-espaces vectoriels $F$ et $G$ de $\mathbb{R}^4$ sont-ils supplémentaires ?

**Réponse**

a) Pour tous nombres réels $x, y, z, t$, il vient

$$\begin{cases} x - y - 2t = 0 \\ x + t = 0 \end{cases} \iff \begin{cases} x - y - 2t = 0 \\ y + 3t = 0 \end{cases} \iff \begin{cases} x = -t \\ y = -3t \end{cases}$$
$$\iff (x, y, z, t) = z(0, 0, 1, 0) + t(-1, -3, 0, 1)$$

et

$$\begin{cases} x - z + t = 0 \\ y + z = 0 \end{cases} \iff \begin{cases} x = z - t \\ y = -z \end{cases} \iff (x, y, z, t) = z(1, -1, 1, 0) + t(-1, 0, 0, 1).$$





Puisqu'on a pratiqué la méthode de Gauss, les vecteurs $u_1 = (0, 0, 1, 0)$ et $u_2 = (-1, -3, 0, 1)$ forment une base de $F$. De même $u_3 = (1, -1, 1, 0)$ et $u_4 = (-1, 0, 0, 1)$ forment une base de $G$.

b) Calculons le déterminant de la matrice dont les colonnes sont les coordonnées des vecteurs $u_1$, $u_2$, $u_3$ et $u_4$ dans la base canonique de $\mathbb{R}^4$. On a

$$\begin{vmatrix} 0 & -1 & 1 & -1 \\ 0 & -3 & -1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{vmatrix} = \begin{vmatrix} -1 & 1 & -1 \\ -3 & -1 & 0 \\ 1 & 0 & 1 \end{vmatrix} = \begin{vmatrix} 0 & 1 & 0 \\ -3 & -1 & 0 \\ 1 & 0 & 1 \end{vmatrix} = \begin{vmatrix} 0 & 1 \\ -3 & -1 \end{vmatrix} = 3.$$

Ce déterminant n'est pas nul, par suite $(u_1, u_2, u_3, u_4)$ est une base de $\mathbb{R}^4$. Les sous-espaces vectoriels $F$ et $G$ de $\mathbb{R}^4$ sont donc supplémentaires.

## Recherche d'une base à partir de vecteurs qui engendrent

Il y a un algorithme pour cela, fondé sur un principe très simple.

Soient $p$ un entier supérieur ou égal à 2 et $u_1, u_2, \ldots, u_p$ des vecteurs de $\mathbf{K}^n$. Notons $F$ le sous-espace vectoriel de $\mathbf{K}^n$ engendré par $u_1, u_2, \ldots, u_p$.

- Soient $a$ un scalaire non nul et $v_1, v_2, \ldots, v_p$ les vecteurs de $F$ définis par $v_1 = au_1$ et $v_i = u_i$ pour tout $i \geqslant 2$. Puisqu'on a $u_1 = (1/a)v_1$, $F$ est le sous espace vectoriel de $\mathbf{K}^n$ engendré par $v_1, v_2, \ldots, v_p$.
- Soient $\lambda$ un scalaire et $w_1, w_2, \ldots, w_p$ les vecteurs de $F$ définis par $w_1 = u_1 + \lambda u_2$ et $w_i = u_i$ pour tout $i \geqslant 2$. Puisqu'on a $u_1 = w_1 - \lambda w_2$, $F$ est le sous-espace vectoriel de $\mathbf{K}^n$ engendré par $w_1, w_2, \ldots, w_p$.

Expliquons cet algorithme sur deux exemples.

**Exemple 1.** Considérons les vecteurs de $\mathbb{R}^4$ : $u_1 = (1, -1, 0, 1)$, $u_2 = (2, 1, 4, 5)$, $u_3 = (1, 2, -4, -2)$, $u_4 = (2, 3, 4, 5)$ et $u_5 = (1, 1, 0, 1)$. Notons $F$ le sous-espace vectoriel de $\mathbb{R}^4$ engendré par ces vecteurs. Écrivons la matrice $A \in M_{4,5}(\mathbb{R})$ dont les coefficients de la $j$-ième colonne sont les coordonnées de $u_j$ dans la base canonique de $\mathbb{R}^4$. Cela revient à écrire en colonnes les coordonnées des vecteurs. Il vient

$$A = \begin{bmatrix} 1 & 2 & 1 & 2 & 1 \\ -1 & 1 & 2 & 3 & 1 \\ 0 & 4 & -4 & 4 & 0 \\ 1 & 5 & -2 & 5 & 1 \end{bmatrix}.$$

La première étape de l'algorithme consiste à remplacer, pour tout $i \geqslant 2$, le vecteur $u_i$ par un vecteur de la forme $u_i - \lambda u_1$ dont la première coordonnée dans la base canonique est nulle.

D'après le principe énoncé, $F$ est ainsi engendré par les vecteurs $v_1 = u_1$, $v_2 = u_2 - 2u_1$, $v_3 = u_3 - u_1$, $v_4 = u_4 - 2u_1$ et $v_5 = u_5 - u_1$.

La matrice dont les colonnes sont les coordonnées de $v_1, v_2, v_3, v_4, v_5$ dans la base canonique de $\mathbb{R}^4$ est

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ -1 & 3 & 3 & 5 & 2 \\ 0 & 4 & -4 & 4 & 0 \\ 1 & 3 & -3 & 3 & 0 \end{bmatrix}.$$

Poursuivons de la manière suivante. Le sous-espace vectoriel $F$ est engendré par les vecteurs $w_1 = v_1$, $w_2 = \frac{1}{2}v_5$, $w_3 = v_3$, $w_4 = v_4$ et $w_5 = v_2$. La matrice dont les colonnes sont les coordonnées de $w_1, w_2, w_3, w_4, w_5$ dans la base canonique de $\mathbb{R}^4$ est

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ -1 & 1 & 3 & 5 & 3 \\ 0 & 0 & -4 & 4 & 4 \\ 1 & 0 & -3 & 3 & 3 \end{bmatrix}.$$

On continue en faisant des opérations élémentaires sur les colonnes de la matrice ci-dessus, jusqu'à obtenir une matrice dont le premier coefficient non nul de chaque colonne est situé en-dessous du premier coefficient non nul de la colonne précédente. On obtient successivement les matrices

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & -4 & 4 & 4 \\ 1 & 0 & -3 & 3 & 3 \end{bmatrix}, \text{ puis } \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & -4 & 0 & 0 \\ 1 & 0 & -3 & 0 & 0 \end{bmatrix}.$$

D'après le principe énoncé, $F$ est engendré par les vecteurs

$$t_1 = (1, -1, 0, 0), \quad t_2 = (0, 1, 0, 0) \quad \text{et} \quad t_3 = (0, 0, 4, 3).$$

Soient $a, b, c$ des nombres réels tels que $at_1 + bt_2 + ct_3 = 0$. Puisque $at_1 + bt_2 + ct_3 = (a, -a + b, 4c, 3c)$, il vient $a = b = c = 0$. Les vecteurs $t_1, t_2, t_3$ sont donc linéairement indépendants et forment ainsi une base de $F$.

**Exemple 2.** Soit $F$ le sous-espace vectoriel de $\mathbb{R}^4$ engendré par les vecteurs $u_1 = (1, 2, 3, 1)$, $u_2 = (1, 1, 2, 0)$ et $u_3 = (2, 2, 1, 3)$. Notons $A$ la matrice de $M_{4,3}(\mathbb{R})$ dont les coefficients de la $j$-ième colonne sont les coordonnées de $u_j$ dans la base canonique de $\mathbb{R}^4$. Il vient

$$A = \begin{bmatrix} 1 & 1 & 2 \\ 2 & 1 & 2 \\ 3 & 2 & 1 \\ 1 & 0 & 3 \end{bmatrix}.$$

Faisons des opérations élémentaires sur les colonnes de la matrice $A$, jusqu'à obtenir une matrice dont le premier coefficient non nul de chaque colonne est situé en-dessous du premier coefficient non nul de la colonne précédente. On obtient





successivement les matrices

$$\begin{bmatrix} 1 & 0 & 2 \\ 2 & -1 & 2 \\ 3 & -1 & 1 \\ 1 & -1 & 3 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 \\ 2 & -1 & -2 \\ 3 & -1 & -5 \\ 1 & -1 & 1 \end{bmatrix} \quad \text{et} \quad \begin{bmatrix} 1 & 0 & 0 \\ 2 & -1 & 0 \\ 3 & -1 & -3 \\ 1 & -1 & 3 \end{bmatrix}.$$

D'après le principe énoncé, $F$ est engendré par les vecteurs

$$v_1 = (1, 2, 3, 1), \quad v_2 = (0, 1, 1, 1) \quad \text{et} \quad v_3 = (0, 0, -1, 1).$$

Si $a, b, c$ sont des nombres réels tels que $av_1 + bv_2 + cv_3 = 0$, il vient $a = b = c = 0$. Les vecteurs $v_1, v_2, v_3$ sont donc linéairement indépendants et forment ainsi une base de $F$. En particulier, on a $\dim F = 3$. Puisque les vecteurs $u_1, u_2, u_3$ engendrent $F$, on en déduit que les vecteurs $u_1, u_2, u_3$ sont linéairement indépendants.

> Appliquer cet algorithme, c'est pratiquer la méthode de Gauss sur les colonnes de la matrice $A$.
> - Les vecteurs non nuls obtenus à la fin de l'algorithme sont linéairement indépendants et forment une base de $F$.
> - Si l'on a $p$ vecteurs de $\mathbb{K}^n$ et si $p \leqslant n$, la méthode de Gauss permet de savoir si ces $p$ vecteurs sont linéairement indépendants.

En particulier, la méthode de Gauss permet de savoir si $n$ vecteurs de $\mathbb{K}^n$ forment une base de $\mathbb{K}^n$.

## Passage de base à équations

Montrons sur un exemple comment pratiquer l'algorithme précédent pour trouver des équations d'un sous-espace vectoriel de $\mathbb{K}^n$, lorsqu'on en connaît une base.

**Exemple.** Soit $F$ le sous-espace vectoriel de $\mathbb{R}^4$ engendré par les vecteurs $u_1 = (1, 1, 2, 1)$ et $u_2 = (2, 1, 3, 4)$. Le vecteur $u_1$ n'est pas nul et le vecteur $u_2$ n'est pas colinéaire à $u_1$, par suite $u_1$ et $u_2$ sont linéairement indépendants et forment ainsi une base de $F$. On en déduit $\dim F = 2$.

Soit $u = (x, y, z, t)$ un vecteur de $\mathbb{R}^4$. Notons $G$ le sous-espace vectoriel de $\mathbb{R}^4$ engendré par $u_1$, $u_2$ et $u$. On a donc $F \subset G$. De plus, on a l'égalité $F = G$ si et seulement si $u \in F$.

La matrice dont les colonnes sont les coordonnées de $u_1, u_2, u$ dans la base canonique de $\mathbb{R}^4$ est

$$A = \begin{bmatrix} 1 & 2 & x \\ 1 & 1 & y \\ 2 & 3 & z \\ 1 & 4 & t \end{bmatrix}.$$

Pratiquons la méthode de Gauss sur les colonnes de $A$ pour trouver une base de $G$. Nous obtenons successivement les matrices

$$\begin{bmatrix} 1 & 0 & 0 \\ 1 & -1 & y-x \\ 2 & -1 & z-2x \\ 1 & 2 & t-x \end{bmatrix} \quad \text{et} \quad \begin{bmatrix} 1 & 0 & 0 \\ 1 & -1 & 0 \\ 2 & -1 & z-y-x \\ 1 & 2 & t+2y-3x \end{bmatrix}.$$

Il s'ensuit que si $z-y-x \neq 0$ <u>ou</u> si $t+2y-3x \neq 0$, alors les vecteurs $(1,1,2,1)$, $(0,-1,-1,2)$ et $(0,0,z-y-x,t+2y-3x)$ forment une base de $G$ et l'on a dans ce cas $\dim G = 3$. Il s'ensuit également que si $z-y-x=0$ <u>et</u> si $t+2y-3x=0$, alors les vecteurs $(1,1,2,1)$ et $(0,-1,-1,2)$ forment une base de $G$ et l'on a dans ce cas $\dim G = 2$. Résumons ce que nous venons de démontrer par les équivalences

$$\begin{aligned} u \in F &\iff G = F \\ &\iff \dim G = \dim F \qquad \text{car } F \subset G \\ &\iff \dim G = 2 \qquad \text{car } \dim F = 2 \\ &\iff \begin{cases} z-y-x=0 \\ t+2y-3x=0. \end{cases} \end{aligned}$$

Des équations de $F$ sont donc $x+y-z=0$ et $-3x+2y+t=0$.

## Exercices

**1.** On considère les vecteurs suivants de $\mathbf{C}^3$ :

$$u_1 = (1-i, i, 1+i), \quad u_2 = (-1,1,3) \quad \text{et} \quad u_3 = (1-i, i, i).$$

**a)** Montrer que $(u_1,u_2,u_3)$ est une base de $\mathbf{C}^3$.

**b)** Calculer les coordonnées du vecteur $(1+i,2,i)$ dans la base $(u_1,u_2,u_3)$.

**2.** On considère les vecteurs suivants de $\mathbf{R}^4$ :

$$u_1 = (1,-2,1,2), \quad u_2 = (1,-3,1,2), \quad u_3 = (2,-4,3,4) \quad \text{et} \quad u_4 = (1,-1,2,3).$$

**a)** Montrer que $(u_1,u_2,u_3,u_4)$ est une base de $\mathbf{R}^4$.

**b)** Soient $a,b,c,d$ des nombres réels. Calculer les coordonnées du vecteur $(a,b,c,d)$ dans la base $(u_1,u_2,u_3,u_4)$.

**c)** Calculer les coordonnées, dans la base $(u_1,u_2,u_3,u_4)$, de chacun des vecteurs de la base canonique de $\mathbf{R}^4$.





**3.** Parmi les sous-ensembles suivants de $\mathbf{R}^4$, préciser lesquels sont des sous-espaces vectoriels et lorsque c'est le cas, en donner une base :

**a)** $\{(x,y,z,t) \in \mathbf{R}^4 \mid 3x-y+t=0\}$,

**b)** $\{(x,y,z,t) \in \mathbf{R}^4 \mid x-y+2z+t=1\}$

**c)** $\{(x,y,z,t) \in \mathbf{R}^4 \mid x+t=0 \text{ et } 2x+y-z=0\}$

**d)** $\{(x,y,z,t) \in \mathbf{R}^4 \mid |x+t| = |y|\}$

**e)** $\{(x,y,z,t) \in \mathbf{R}^4 \mid \exists (a,b) \in \mathbf{R}^2,\ (x,y,z,t) = (3a+b, a-b, a+5b, 2a+b)\}$.

**4.** Soit $F$ le sous-espace vectoriel de $\mathbf{R}^4$ engendré par les vecteurs $(0,-1,1,1)$, $(2,1,-1,1)$ et $(1,1,-1,0)$. Soit $G$ le sous-espace vectoriel de $\mathbf{R}^4$ engendré par les vecteurs $(1,3,0,1)$, $(2,4,-2,2)$ et $(-1,-2,1,-1)$. Les sous-espaces vectoriels $F$ et $G$ de $\mathbf{R}^4$ sont-ils supplémentaires ?

**5.** Soit $F$ le sous-espace vectoriel de $\mathbf{R}^3$ engendré par les vecteurs $(2,3,-1)$ et $(1,-1,-2)$. Soit $G$ le sous-espace vectoriel de $\mathbf{R}^3$ engendré par les vecteurs $(3,7,0)$ et $(5,0,-7)$.

**a)** Montrer que l'on a $F = G$.

**b)** Trouver une équation de $F$.

**6.** Soit $a$ un nombre réel. Quel est la dimension du sous-espace vectoriel de $\mathbf{R}^3$ engendré par les vecteurs $(a+2,a,a-2)$, $(1,a,-1)$ et $(a,-a,1)$ ?

**7.** On considère les vecteurs suivants de $\mathbf{R}^4$ :

$$u_1 = (-3,1,0,2), \quad u_2 = (-5,2,1,2), \quad u_3 = (1,1,4,-6) \quad \text{et} \quad u_4 = (-1,0,-1,2).$$

**a)** Montrer que le sous-espace vectoriel de $\mathbf{R}^4$ engendré par $u_1$ et $u_2$ est égal au sous-espace vectoriel de $\mathbf{R}^4$ engendré par $u_3$ et $u_4$.

**b)** Montrer que les vecteurs $u_1$ et $u_2$ sont linéairement indépendants. Compléter ces vecteurs pour former une base de $\mathbf{R}^4$.

**8.** Soit $F$ le sous-espace vectoriel de $\mathbf{R}^5$ engendré par les vecteurs $(1,0,1,-1,0)$, $(2,1,2,1,1)$ et $(3,1,2,0,1)$. Soit $G$ le sous-espace vectoriel de $\mathbf{R}^5$ engendré par les vecteurs $(1,1,3,-1,1)$, $(2,-1,-4,4,-1)$, $(0,1,2,0,1)$ et $(1,-2,-3,-1,-2)$.

**a)** Trouver une base de $F$ et une base de $G$.

**b)** Déterminer une base de $F+G$ et donner une équation de $F+G$.

**c)** Trouver des équations de $F$ et des équations de $G$.

**d)** Déterminer une base de $F \cap G$.

**9.** Soit $a$ un nombre réel et soit $E$ le sous-espace vectoriel de $\mathbb{R}^4$ engendré par les vecteurs $(1, a, 2, -1)$, $(-2, 3, a, 1)$, $(-1, 0, 2, -1)$, $(2, -1, a, 1)$.

**a)** Pour quelle valeur de $a$ a-t-on l'égalité $E = \mathbb{R}^4$ ?

**b)** On suppose $a = -2$.

**(i)** Trouver une base de $E$.

**(ii)** Trouver des équations de $E$.

**(iii)** L'espace vectoriel $E$ contient-il un vecteur de la base canonique ? Le vecteur $(1, -1, 0, 0)$ appartient-il à $E$ ?

**10.** Posons $A = \begin{bmatrix} 2 & -1 & 0 \\ -2 & 1 & 2 \\ 2 & -1 & 0 \end{bmatrix}$, $P = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$ et $D = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix}$.

**a)** Soit $B \in M_3(\mathbb{R})$. Montrer que l'ensemble des matrices $M \in M_3(\mathbb{R})$ telles que $MB = BM$ est un sous-espace vectoriel de $M_3(\mathbb{R})$.

**b)** Donner une base de l'espace vectoriel des matrices $M \in M_3(\mathbb{R})$ telles que $MD = DM$.

**c)** Calculer $P^{-1}AP$. En déduire que pour toute matrice $M \in M_3(\mathbb{R})$, on a $MA = AM$ si et seulement si on a $(P^{-1}MP)D = D(P^{-1}MP)$.

**d)** Trouver une base de l'espace vectoriel des matrices $M \in M_3(\mathbb{R})$ telles que $MA = AM$.

**11.** Trouver des matrices $A$ et $B$ telles que les matrices $A, B, AB, BA$ forment une base de l'espace vectoriel $M_2(\mathbb{R})$.

**12.** Soit $n$ un entier supérieur ou égal à 2.

**a)** L'ensemble des matrices inversibles de $M_n(\mathbf{K})$ est-il un sous-espace vectoriel de $M_n(\mathbf{K})$ ?

**b)** Montrer que l'ensemble des matrices triangulaires supérieures de $M_n(\mathbf{K})$ est un sous-espace vectoriel de $M_n(\mathbf{K})$ et calculer sa dimension.

**13.** Soit $F$ l'ensemble des matrices $A \in M_3(\mathbb{R})$ telles que ${}^tA = A$. Soit $G$ l'ensemble des matrices $A \in M_3(\mathbb{R})$ telles que ${}^tA = -A$.

**a)** Montrer que $F$ et $G$ sont des sous-espaces vectoriels de $M_3(\mathbb{R})$. Calculer leur dimension.

**b)** Montrer que $F$ et $G$ sont des sous-espaces vectoriels supplémentaires de $M_3(\mathbb{R})$.

**14.** Soient $E$ le $\mathbb{R}$-espace vectoriel des suites à termes réels et $a$ un nombre réel non nul. On considère $F$ l'ensemble des suites $(u_n)$ de $E$ telles que $u_{n+1} = au_n$ pour tout entier naturel $n$.

**a)** Montrer que $F$ est un sous-espace vectoriel de $E$.

**b)** Soit $(u_n)$ une suite appartenant à $F$. Montrer que l'on a $u_n = u_0 a^n$ pour tout entier naturel $n$.

**c)** En déduire que $F$ est une droite vectorielle.





**15.** Soient $E$ le $\mathbb{C}$-espace vectoriel des suites à termes complexes et $a, b$ des nombres complexes. On considère $F$ l'ensemble des suites $(u_n)$ de $E$ telles que $u_{n+2} = au_{n+1} + bu_n$ pour tout $n \in \mathbb{N}$.

**a)** Montrer que $F$ est un sous-espace vectoriel de $E$.

**b)** Soit $r$ un nombre complexe. Montrer que la suite $(r^n)$ appartient à $F$ si et seulement si $r^2 = ar + b$.

**16.** Poursuivons l'exercice précédent en supposant $a = 2$ et $b = -5$.

**a)** Trouver deux nombres complexes $\alpha$ et $\beta$ tels que les suites $(\alpha^n)$ et $(\beta^n)$ appartiennent à $F$.

**b)** Soient $(u_n)$ et $(v_n)$ des suites appartenant à $F$ telles que $u_0 = v_0$ et $u_1 = v_1$. Montrer que l'on a $u_n = v_n$ pour tout $n \in \mathbb{N}$.

**c)** Soit $(u_n)$ une suite appartenant à $F$. Montrer qu'il existe des nombres complexes $\lambda$ et $\mu$ uniques tels que $u_n = \lambda\alpha^n + \mu\beta^n$ pour tout $n \in \mathbb{N}$.

**d)** Quelle est la dimension de $F$ ?

**e)** Calculer explicitement le terme général de la suite $(u_n)$ appartenant à $F$ telle que $u_0 = 1$ et $u_1 = i$.

**17.** Soit $E$ le $\mathbb{R}$-espace vectoriel des fonctions de $\mathbb{R}$ dans $\mathbb{R}$. Soient $F$ l'ensemble des fonctions paires de $\mathbb{R}$ dans $\mathbb{R}$ et $G$ l'ensemble des fonctions impaires de $\mathbb{R}$ dans $\mathbb{R}$.

**a)** Montrer que $F$ et $G$ sont des sous-espaces vectoriels de $E$.

**b)** Montrer que $F$ et $G$ sont des sous-espaces vectoriels supplémentaires de $E$.

**c)** Notons exp la fonction exponentielle. D'après la question précédente, il existe des fonctions $f$ et $g$ uniques telles que $\exp = f + g$, $f \in F$ et $g \in G$. Reconnaître les fonctions usuelles $f$ et $g$.

**18.** Soient $u = (a, b, c)$ et $u' = (a', b', c')$ des vecteurs non nuls de $\mathbb{R}^3$.

**a)** Montrer que si le vecteur $u'$ est colinéaire à $u$, alors on a $\begin{vmatrix} a & a' \\ b & b' \end{vmatrix} = \begin{vmatrix} b & b' \\ c & c' \end{vmatrix} = \begin{vmatrix} a & a' \\ c & c' \end{vmatrix} = 0$.

**b)** On suppose que l'on a $\begin{vmatrix} a & a' \\ b & b' \end{vmatrix} = \begin{vmatrix} b & b' \\ c & c' \end{vmatrix} = \begin{vmatrix} a & a' \\ c & c' \end{vmatrix} = 0$. Montrer que le vecteur $u'$ est colinéaire à $u$.

**19.** Soit $E$ un K-espace vectoriel de dimension $n \geqslant 3$. Soit $F$ un sous-espace vectoriel de $E$ de dimension $n - 2$ et soit $G$ un supplémentaire de $F$.

**a)** Quelle est la dimension de $G$ ?

**b)** Soient $(u, v)$ une base de $G$, $f$ un vecteur de $F$ et $G'$ le sous-espace vectoriel de $E$ engendré par les vecteurs $u + f$ et $v + f$.

**(i)** Quelle est la dimension de $G'$ ?

**(ii)** Montrer que les sous-espaces $F$ et $G'$ sont supplémentaires.

**c)** En déduire qu'il existe plusieurs sous-espaces supplémentaires de $F$.

**20.** Notons $E$ le $\mathbf{R}$-espace vectoriel des fonctions de $\mathbf{R}$ dans $\mathbf{R}$.

**a)** Soient $f_1, f_2 \in E$. On suppose que les fonctions $f_1$ et $f_2$ sont linéairement indépendantes. Montrer qu'il existe $x_1 \in \mathbf{R}$ tel que $f_1(x_1) \neq 0$ et que la fonction $f : \mathbf{R} \to \mathbf{R}$ définie par

$$f(x) = \begin{vmatrix} f_1(x_1) & f_1(x) \\ f_2(x_1) & f_2(x) \end{vmatrix}$$

n'est pas nulle.

**b)** Soient $f_1, f_2 \in E$. Montrer que les fonctions $f_1$ et $f_2$ sont linéairement indépendantes si et seulement s'il existe des nombres réels $x_1$ et $x_2$ tels que

$$\begin{vmatrix} f_1(x_1) & f_1(x_2) \\ f_2(x_1) & f_2(x_2) \end{vmatrix} \neq 0.$$

**c)** Soient $f_1, f_2, f_3 \in E$. On suppose que les fonctions $f_1$, $f_2$ et $f_3$ sont linéairement indépendantes. Montrer qu'il existe $x_1, x_2 \in \mathbf{R}$ tels que $\begin{vmatrix} f_1(x_1) & f_1(x_2) \\ f_2(x_1) & f_2(x_2) \end{vmatrix} \neq 0$. On considère la fonction $g : \mathbf{R} \to \mathbf{R}$ définie par

$$g(x) = \begin{vmatrix} f_1(x_1) & f_1(x_2) & f_1(x) \\ f_2(x_1) & f_2(x_2) & f_2(x) \\ f_3(x_1) & f_3(x_2) & f_3(x) \end{vmatrix}.$$

Montrer que la fonction $g$ est combinaison linéaire de $f_1$, $f_2$ et $f_3$. En déduire que $g$ n'est pas la fonction nulle.

**d)** Soient $f_1, f_2, f_3 \in E$. Montrer que les fonctions $f_1$, $f_2$ et $f_3$ sont linéairement indépendantes si et seulement s'il existe des nombres réels $x_1$, $x_2$ et $x_3$ tels que

$$\begin{vmatrix} f_1(x_1) & f_1(x_2) & f_1(x_3) \\ f_2(x_1) & f_2(x_2) & f_2(x_3) \\ f_3(x_1) & f_3(x_2) & f_3(x_3) \end{vmatrix} \neq 0.$$

## Quelques réponses ou indications

2. **b)** Les coordonnées de $(a, b, c, d)$ dans la base $(u_1, u_2, u_3, u_4)$ sont $5a + b - 2c$, $-4a - b + d$, $a + c - d$, $-2a + d$.

**c)** Utiliser **(b)**.

3. Les sous-espaces vectoriels de $\mathbf{R}^4$ sont les sous-ensembles définis en **(a)**, **(c)** et **(e)** et sont de dimension respective 3, 2 et 2.

4. Chercher une base de $F$ et une base de $G$.

5. Démontrer que $\dim F = \dim G$ et que l'on a par exemple $F \subset G$.





6. La dimension est égale à 3 si $a$ est différent de 0,1 et $-1$. Elle est égale à 2 si $a$ est égal à 0, 1 ou $-1$.

8. **d)** Les vecteurs de $F \cap G$ sont ceux qui vérifient les équations de $F$ et les équations de $G$.

9. **a)** Le déterminant dont les colonnes sont les coordonnées des vecteurs est égal à $4(a+2)^2$. On a donc $E = \mathbf{R}^4$ si et seulement si $a \neq -2$.

**b)** (i) On trouve une base formée de deux vecteurs.

(ii) Des équations de $E$ sont par exemple $\begin{cases} 2x + 2y + z = 0 \\ x + y - t = 0. \end{cases}$

(iii) Utiliser des équations de $E$ pour répondre aux questions.

10. **b)** On doit trouver une base formée de trois éléments.

**c)** On a $P^{-1}AP = D$.

**d)** Utiliser les deux questions précédentes.

12. **a)** Non, car la matrice nulle n'appartient pas à l'ensemble en question.

**b)** Trouver une base de cet espace vectoriel ; la dimension est égale à $n(n+1)/2$.

13. **b)** Montrer que $F \cap G = \{0\}$ et calculer la dimension de $F + G$.

14. **c)** La suite $(a^n)$ est une base de $F$.

16. **b)** Raisonner par récurrence.

**c)** Puisque $F$ est un espace vectoriel, la suite $\lambda(\alpha^n) + \mu(\beta^n) = (\lambda\alpha^n + \mu\beta^n)$ appartient à $F$. Montrer qu'il existe des nombres complexes $\lambda$ et $\mu$ uniques tels que $u_0 = \lambda + \mu$ et $u_1 = \lambda\alpha + \mu\beta$. Conclure en utilisant **(b)**.

**d)** D'après **(c)**, les suites $(\alpha^n)$ et $(\beta^n)$ forment une base de $F$. On a donc $\dim F = 2$.

**e)** On a $u_n = \frac{1}{4}(3+i)(1+2i)^n + \frac{1}{4}(1-i)(1-2i)^n$.

17. **b)** Montrer que $F \cap G = \{0\}$. Soit $h \in E$. Pour trouver $f \in F$ et $g \in G$ telles que $h = f + g$, écrire $h(x) = f(x) + g(x)$ et $h(-x) = f(-x) + g(-x) = f(x) - g(x)$ pour tout $x \in \mathbf{R}$.

**c)** On a $f(x) = \operatorname{ch}(x)$ et $g(x) = \operatorname{sh}(x)$.

18. **b)** Considérer les vecteurs $a'u - au'$, $b'u - bu'$ et $c'u - cu'$.

19. **a)** La dimension de $G$ est égale à 2.

**b)** (i) Montrer que les vecteurs $u + f$ et $v + f$ sont linéairement indépendants.

**c)** Montrer que si $f \neq 0$, alors $G \neq G'$.

20. **a)** Puisque les fonctions $f_1$ et $f_2$ sont linéairement indépendantes, la fonction $f_1$ n'est pas nulle, donc il existe $x_1 \in \mathbf{R}$ tel que $f_1(x_1) \neq 0$. Posons $\lambda_1 = -f_2(x_1)$ et $\lambda_2 = f_1(x_1)$. Alors on a $f = \lambda_1 f_1 + \lambda_2 f_2$ et $\lambda_2 \neq 0$. Les fonctions $f_1$ et $f_2$ étant linéairement indépendantes, la fonction $f$ n'est pas la fonction nulle.

**b)** Utiliser **(a)** pour démontrer l'existence de $x_1$ et $x_2$. Réciproquement, considérer des nombres réels $\lambda$ et $\mu$ tels que $\lambda f_1 + \mu f_2 = 0$, autrement dit tels que $\lambda f_1 + \mu f_2$ est la fonction nulle. En particulier les valeurs de cette fonction en $x_1$ et en $x_2$ sont nulles. En déduire $\lambda = \mu = 0$.

# Chapitre 7

# Applications linéaires

Après la notion d'espace vectoriel, voici celle d'*application linéaire*. Dans le cadre des espaces vectoriels de dimension finie, applications linéaires et matrices ont des liens très étroits qui justifient le calcul matriciel. Dans ce chapitre, la lettre $\mathbf{K}$ désigne $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.

## 1. Définitions et premières propriétés

Dans ce paragraphe, $E$ et $F$ sont des $\mathbf{K}$-espaces vectoriels.

**Définitions**

Une *application linéaire* de $E$ dans $F$ est une application $f:E\to F$ telle que $f(x+y)=f(x)+f(y)$ pour tous $x,y\in E$ et $f(\lambda x)=\lambda f(x)$ pour tout $x\in E$ et pour tout $\lambda\in\mathbf{K}$. Si $F=\mathbf{K}$, on dit que $f$ est une *forme linéaire* sur $E$.

Si l'on fait $\lambda=0$ dans l'égalité $f(\lambda x)=\lambda f(x)$, alors il vient $f(0)=0$.
De plus, si $x_1,\dots,x_n$ sont des vecteurs appartenant à $E$ et si $\lambda_1,\dots,\lambda_n$ sont des scalaires, alors on a $f(\lambda_1x_1+\cdots+\lambda_nx_n)=\lambda_1f(x_1)+\cdots+\lambda_nf(x_n)$. Cette égalité se démontre par récurrence sur $n$.

**Exemples**

- Soit $f$ une application de $\mathbf{K}$ dans $E$. L'application $f$ est linéaire si et seulement s'il existe un vecteur $e\in E$ tel que $f(x)=xe$ pour tout $x\in\mathbf{K}$. En effet, si l'on a $f(x)=xe$ pour tout $x\in\mathbf{K}$, il est clair que l'application $f$ est linéaire. Réciproquement, si l'application $f$ est linéaire, il suffit de poser $e=f(1)$.
- L'application identique de $E$ est une application linéaire de $E$ dans $E$. On rappelle que cette application est notée $\mathrm{id}_E$ et que l'on a par définition $\mathrm{id}_E(x)=x$ pour tout $x\in E$.

- Soient $n, p$ des entiers positifs et $A$ une matrice appartenant à $M_{n,p}(\mathbf{K})$. D'après les règles du calcul matriciel, si $q$ est un entier positif (en particulier si $q = 1$), alors l'application $f : M_{p,q}(\mathbf{K}) \to M_{n,q}(\mathbf{K})$ définie par $f(X) = AX$ pour toute matrice $X \in M_{p,q}(\mathbf{K})$, est linéaire.
- Si $E$ est l'espace vectoriel des fonctions de classe $C^\infty$ (voir le chapitre 11 du tome d'analyse) sur un intervalle $I$ de $\mathbf{R}$ et à valeurs dans $\mathbf{R}$, alors l'application de $E$ dans $E$ qui à toute fonction $f \in E$ associe sa dérivée $f'$ est linéaire.
- Soient $a, b$ des nombres réels tels que $a < b$. Si $E$ est l'espace vectoriel des fonctions continues sur $[a,b]$, alors l'application $\varphi : E \to \mathbf{R}$ qui à tout $f \in E$ associe $\varphi(f) = \int_a^b f(t)\,dt$ est une forme linéaire. Cela résulte des propriétés de l'intégrale (voir le chapitre 9 du tome d'analyse).

**Proposition.** *Soient $f$ et $g$ des applications linéaires de $E$ dans $F$ et soit $\lambda \in \mathbf{K}$. Les applications $f + g : E \to F$ et $\lambda f : E \to F$ définies par $(f+g)(x) = f(x) + g(x)$ et $(\lambda f)(x) = \lambda f(x)$ pour tout $x \in E$ sont linéaires.*

**Démonstration.** Soient $x$ et $y$ des vecteurs de $E$. On a

$$\begin{aligned}(f+g)(x+y) &= f(x+y) + g(x+y) && \text{par définition de } f+g\\ &= f(x) + f(y) + g(x) + g(y) && \text{puisque } f \text{ et } g \text{ sont linéaires}\\ &= (f+g)(x) + (f+g)(y).\end{aligned}$$

De même on démontre que pour tout $\mu \in \mathbf{K}$, on a $(f+g)(\mu x) = \mu(f+g)(x)$. Il s'ensuit que l'application $f + g$ est linéaire. On démontre de la même manière que l'application $\lambda f$ est linéaire. ∎

Voici des applications linéaires utiles en géométrie.

**Homothétie.** Soit $\lambda \in \mathbf{K}$. L'application linéaire $f = \lambda\,\mathrm{id}_E$ s'appelle l'*homothétie* de rapport $\lambda$. On a donc $f(x) = \lambda x$ pour tout $x \in E$.

**Projection et symétrie**

Soient $E_1$ et $E_2$ des sous-espaces vectoriels supplémentaires de $E$. On rappelle que tout vecteur $x \in E$ s'écrit de manière unique $x = x_1 + x_2$, où $x_1 \in E_1$ et $x_2 \in E_2$.

- Soit $p : E \to E$ l'application définie $p(x) = x_1$ pour tout $x \in E$. Pour tout $\lambda \in \mathbf{K}$, on a $\lambda x = \lambda x_1 + \lambda x_2$, $\lambda x_1 \in E_1$ et $\lambda x_2 \in E_2$, donc $p(\lambda x) = \lambda x_1 = \lambda p(x)$. De même on a $p(x+y) = p(x) + p(y)$. L'application $p$ est donc linéaire. On l'appelle la *projection sur $E_1$ parallèlement à $E_2$*. Remarquons que l'on a

$$p(x) = 0 \text{ si et seulement si } x \in E_2 \quad \text{et} \quad p(x) = x \text{ si et seulement si } x \in E_1.$$



- Soit $s : E \to E$ l'application définie $s(x) = x_1 - x_2$. Pour tout $x \in E$, on a

$$s(x) = x_1 - x_2 = 2x_1 - (x_1 + x_2) = 2p(x) - x = (2p - \mathrm{id}_E)(x),$$

autrement dit $s = 2p - \mathrm{id}_E$. L'application $s$ donc est linéaire. On l'appelle la *symétrie par rapport à $E_1$ parallèlement à $E_2$*. Remarquons que l'on a

$$s(x) = -x \text{ si et seulement si } x \in E_2 \quad \text{et} \quad s(x) = x \text{ si et seulement si } x \in E_1.$$

**Exemples**

- Soit $f : \mathbf{R}^2 \to \mathbf{R}^2$ l'application définie par $f(x,y) = (4x - 2y, 6x - 3y)$, pour tous $x, y \in \mathbf{R}$. Si $x, y$ sont des nombres réels, on a

$$(x,y) = (4x - 2y, 6x - 3y) + (-3x + 2y, -6x + 4y) = (2x - y)(2,3) + (2y - 3x)(1,2).$$

Notons $E_1$ la droite de $\mathbf{R}^2$ engendrée par le vecteur $(2,3)$ et $E_2$ la droite de $\mathbf{R}^2$ engendrée par le vecteur $(1,2)$. Puisque ces vecteurs sont linéairement indépendants, on a $\mathbf{R}^2 = E_1 \oplus E_2$. L'application $f$ est donc la projection sur $E_1$ parallèlement à $E_2$.
- Notons maintenant $E_1$ la droite de $\mathbf{R}^2$ engendrée par $(1,1)$ et $E_2$ la droite engendrée par $(1,-1)$. On a $\mathbf{R}^2 = E_1 \oplus E_2$ et pour tous $x, y \in \mathbf{R}$

$$(x,y) = \frac{x+y}{2}(1,1) + \frac{x-y}{2}(1,-1) \quad \text{et} \quad (y,x) = \frac{x+y}{2}(1,1) - \frac{x-y}{2}(1,-1).$$

Par suite l'application $g : \mathbf{R}^2 \to \mathbf{R}^2$ définie par $g(x,y) = (y,x)$ est la symétrie par rapport à $E_1$ parallèlement à $E_2$.

**Définition**

Soit $n$ un entier supérieur ou égal à 2. Si $f$ est une application de $E$ dans $\mathbf{K}^n$, les *composantes* de $f$ sont les applications $f_1, f_2, \ldots, f_n$ de $E$ dans $\mathbf{K}$ définies par $f(x) = (f_1(x), f_2(x), \ldots, f_n(x))$ pour tout $x \in E$.

**Proposition.** *Soit $n$ un entier supérieur ou égal à 2. Si $f$ est une application de $E$ dans $\mathbf{K}^n$, alors l'application $f$ est linéaire si et seulement si ses composantes $f_1, f_2, \ldots, f_n$ sont des formes linéaires.*

**Démonstration.** Soient $x$, $y$ des vecteurs de $E$ et $\lambda$ un élément de $\mathbf{K}$. Par définition des composantes de $f$, on a $f(x+y) = (f_1(x+y), f_2(x+y), \ldots, f_n(x+y))$ et $f(\lambda x) = (f_1(\lambda x), f_2(\lambda x), \ldots, f_n(\lambda x))$. De plus, d'après les règles de calcul dans un espace vectoriel produit, on a $f(x) + f(y) = (f_1(x) + f_1(y), f_2(x) + f_2(y), \ldots, f_n(x) + f_n(y))$ et $\lambda f(x) = (\lambda f_1(x), \lambda f_2(x), \ldots, \lambda f_n(x))$. On en déduit que l'application $f$ est linéaire si et seulement si $f_1, f_2, \ldots, f_n$ sont des applications linéaires, c'est-à-dire des formes linéaires puisque ce sont des applications à valeurs dans $\mathbf{K}$. ∎

**Théorème.** *Supposons $E$ de dimension $n \geqslant 1$. Soient $(e_1, \dots, e_n)$ une base de $E$ et $u_1, \dots, u_n$ des vecteurs de $F$. Soit $f : E \to F$ l'application définie par $f(x) = x_1u_1 + \cdots + x_nu_n$ pour tout $x \in E$, où $x_1, \dots, x_n$ sont les coordonnées de $x$ dans la base $(e_1, \dots, e_n)$. Alors l'application $f$ est linéaire. De plus, $f$ est l'unique application linéaire de $E$ dans $F$ telle que $f(e_i) = u_i$ pour tout $i \in \{1, \dots, n\}$.*

**Démonstration.** Soient $x, y \in E$ et $\lambda \in \mathbf{K}$. Notons $x_1, \dots, x_n$ et $y_1, \dots, y_n$ les scalaires tels que $x = x_1e_1 + \cdots + x_ne_n$ et $y = y_1e_1 + \cdots + y_ne_n$. Il vient $x + y = (x_1 + y_1)e_1 + \cdots + (x_n + y_n)e_n$ et $\lambda x = \lambda x_1e_1 + \cdots + \lambda x_ne_n$. On en déduit $f(\lambda x) = \lambda x_1u_1 + \cdots + \lambda x_nu_n = \lambda f(x)$ et

$$\begin{aligned} f(x + y) &= (x_1 + y_1)u_1 + \cdots + (x_n + y_n)u_n \\ &= (x_1u_1 + \cdots + x_nu_n) + (y_1u_1 + \cdots + y_nu_n) = f(x) + f(y). \end{aligned}$$

L'application $f$ est donc linéaire et par définition de $f$, on a $f(e_i) = u_i$ pour tout $i \in \{1, \dots, n\}$.

Démontrons l'unicité de $f$. Pour cela, supposons que $g : E \to F$ est une application linéaire vérifiant aussi $g(e_i) = u_i$ pour tout $i \in \{1, \dots, n\}$. Puisque l'application $g$ est linéaire, on a pour tous $x_1, \dots, x_n \in \mathbf{K}$,

$$g(x_1e_1 + \cdots + x_ne_n) = x_1g(e_1) + \cdots + x_ng(e_n) = x_1u_1 + \cdots + x_nu_n.$$

Il s'ensuit $f(x_1e_1 + \cdots + x_ne_n) = g(x_1e_1 + \cdots + x_ne_n)$ pour tous $x_1, \dots, x_n \in \mathbf{K}$ et donc $g(x) = f(x)$ pour tout $x \in E$, puisque $E$ est engendré par les vecteurs $e_1, \dots, e_n$. Cela signifie que $g = f$. ■

Le théorème précédent est important : il donne un procédé pour construire des applications linéaires. De plus, il met en évidence le résultat suivant, qui est d'une grande utilité.

> Si $E$ est de dimension finie, deux applications linéaires $f$ et $g$ de $E$ dans $F$ sont égales si et seulement si elles coïncident sur chaque vecteur d'une base de $E$.

**Proposition.** *Soit $n$ un entier positif et soit $f : \mathbf{K}^n \to \mathbf{K}$ une application. L'application $f$ est linéaire si et seulement s'il existe $a_1, \dots, a_n \in \mathbf{K}$ tels que*

$$f(x_1, \dots, x_n) = a_1x_1 + \cdots + a_nx_n \quad \textit{pour tous} \quad x_1, \dots, x_n \in \mathbf{K}.$$

**Démonstration.** Notons $(\mathrm{e}_1, \dots, \mathrm{e}_n)$ la base canonique de $\mathbf{K}^n$. Puisque les coordonnées du vecteur $(x_1, \dots, x_n)$ de $\mathbf{K}^n$ dans la base $(\mathrm{e}_1, \dots, \mathrm{e}_n)$ sont $x_1, \dots, x_n$, s'il existe de tels scalaires $a_1, \dots, a_n$, alors l'application $f$ est linéaire d'après le théorème précédent. Réciproquement, supposons que $f$ une forme linéaire sur $\mathbf{K}^n$.





Posons $a_i = f(\mathrm{e}_i)$ pour tout $i \in \{1, 2, \dots, n\}$. D'après le théorème précédent, l'application $g : \mathbf{K}^n \to \mathbf{K}$ définie par $g(x_1, \dots, x_n) = a_1x_1 + \cdots + a_nx_n$ est linéaire et l'on a $f = g$. ■

Si $n$ et $p$ sont des entiers positifs, on sait que les applications linéaires de $\mathbf{K}^n$ dans $\mathbf{K}^p$ sont les applications dont chaque composante est une forme linéaire sur $\mathbf{K}^n$. Grâce à cette dernière proposition, nous sommes donc en mesure de décrire toutes les applications linéaires de $\mathbf{K}^n$ dans $\mathbf{K}^p$.

Par exemple, une application linéaire de $\mathbb{R}^2$ dans $\mathbb{R}^2$ est une application de la forme $(x, y) \mapsto (ax + by, cx + dy)$, où $a, b, c, d$ sont des nombres réels.

Intéressons-nous maintenant aux applications linéaires bijectives et en particulier cherchons à les caractériser.

**Définition**

Un *isomorphisme* de $E$ sur $F$ est une application linéaire de $E$ dans $F$ qui est bijective.

**Proposition.** *Si $f$ est un isomorphisme de $E$ sur $F$, alors la bijection réciproque $f^{-1}$ est un isomorphisme de $F$ sur $E$.*

**Démonstration.** L'application $f^{-1}$ est bijective (voir chapitre 2). Il reste donc à montrer que l'application $f^{-1}$ est linéaire. Soient $y, y' \in F$. Puisque l'application $f$ est bijective, il existe $x, x' \in E$ uniques, tels que $f(x) = y$ et $f(x') = y'$. Par définition de l'application $f^{-1}$, il vient $x = f^{-1}(y)$ et $x' = f^{-1}(y')$, donc $x + x' = f^{-1}(y) + f^{-1}(y')$. L'application $f$ étant linéaire, on en déduit $f(x + x') = f(x) + f(x')$, c'est-à-dire $f(x + x') = y + y'$. Le vecteur $x + x'$ de $E$ est ainsi l'unique antécédent par $f$ du vecteur $y + y'$ ; il s'ensuit $f^{-1}(y + y') = x + x'$, c'est-à-dire $f^{-1}(y + y') = f^{-1}(y) + f^{-1}(y')$. De la même manière, on démontre que si $\lambda$ est un scalaire de $\mathbf{K}$, alors $f^{-1}(\lambda y) = \lambda f^{-1}(y)$. L'application $f^{-1}$ est donc linéaire. ■

**Définition**

On dit que $E$ et $F$ sont *isomorphes* ou que $E$ est *isomorphe* à $F$, s'il existe un isomorphisme de $E$ sur $F$.

**Proposition.** *Supposons $E$ de dimension $n \geqslant 1$. Soit $(e_1, \dots, e_n)$ une base de $E$ et soit $f : E \to F$ une application linéaire. L'application $f$ est un isomorphisme si et seulement si $(f(e_1), \dots, f(e_n))$ est une base de $F$.*

**Démonstration.** Supposons que $(f(e_1), \dots, f(e_n))$ est une base de $F$. Soit $x \in E$, de coordonnées $x_1, \dots, x_n$ dans la base $(e_1, \dots, e_n)$. On a $x = x_1e_1 + \cdots + x_ne_n$, donc $f(x) = x_1f(e_1) + \cdots + x_nf(e_n)$. Les coordonnées de $f(x)$ dans la base $(f(e_1), \dots, f(e_n))$

sont donc $x_1, \ldots, x_n$. Il s'ensuit que si $x$ et $x'$ sont des vecteurs de $E$ tels que $f(x) = f(x')$, alors $x$ et $x'$ ont les mêmes coordonnées dans la base $(e_1, \ldots, e_n)$, par suite $x = x'$. L'application $f$ est donc injective. Soit $y \in F$ de coordonnées $y_1, \ldots, y_n$ dans la base $\big(f(e_1), \ldots, f(e_n)\big)$. Le vecteur $x = y_1 e_1 + \cdots + y_n e_n$ a pour image $y$ par $f$, par suite $f$ est surjective.

Réciproquement, supposons que $f$ est un isomorphisme. Soit $y \in F$. Puisque $f$ est surjective, il existe $x \in E$ tel que $y = f(x)$. Si $x_1, \ldots, x_n$ sont les coordonnées de $x$ dans la base $(e_1, \ldots, e_n)$, on a $y = f(x_1 e_1 + \cdots + x_n e_n) = x_1 f(e_1) + \cdots + x_n f(e_n)$. L'espace vectoriel $F$ est donc engendré par $f(e_1), \ldots, f(e_n)$. Soient $\lambda_1, \ldots, \lambda_n$ des scalaires tels que $\lambda_1 f(e_1) + \cdots + \lambda_n f(e_n) = 0$. Il vient $f(\lambda_1 e_1 + \cdots + \lambda_n e_n) = 0 = f(0)$. Puisque $f$ est injective, il s'ensuit $\lambda_1 e_1 + \cdots + \lambda_n e_n = 0$. Or les coordonnées du vecteur nul dans la base $(e_1, \ldots, e_n)$ sont toutes nulles, par suite $\lambda_1 = \cdots = \lambda_n = 0$. Les vecteurs $f(e_1), \ldots, f(e_n)$ sont donc linéairement indépendants. ∎

**Corollaire.** *Supposons $E$ et $F$ de dimension finie. Alors $E$ et $F$ sont isomorphes si et seulement si* $\dim E = \dim F$.

**Démonstration.** Le résultat est clair si $E = \{0\}$. Supposons $E \neq \{0\}$ et posons $n = \dim E$. Soit $(e_1, \ldots, e_n)$ une base de $E$.

Si $f$ est un isomorphisme de $E$ sur $F$, alors $\big(f(e_1), \ldots, f(e_n)\big)$ est une base de $F$, d'après la proposition précédente. On a donc $\dim F = n$.

Supposons $\dim F = n$ et donnons-nous $(u_1, \ldots, u_n)$ une base de $F$. Soit $g : E \to F$ l'unique application linéaire telle que $g(e_i) = u_i$ pour tout $i \in \{1, \ldots, n\}$. Alors $g$ est un isomorphisme, d'après la proposition précédente. ∎

En particulier, si $n$ est un entier positif, alors $E$ est de dimension $n$ si et seulement si $E$ est isomorphe à $\mathbf{K}^n$. Ainsi $\mathbf{K}^n$ est un exemple fondamental d'espace vectoriel.

Montrons pour terminer ce paragraphe qu'une composée d'applications linéaires est linéaire.

**Proposition.** *Soit $G$ un $\mathbf{K}$-espace vectoriel. Si $f : E \to F$ et $g : F \to G$ sont des applications linéaires, alors la composée $g \circ f$ est une application linéaire de $E$ dans $G$.*

**Démonstration.** Soient $x, y \in E$. Puisque l'application $f$ est linéaire, on a $f(x + y) = f(x) + f(y)$. L'application $g$ étant également linéaire, il vient $g\big(f(x + y)\big) = g\big(f(x)\big) + g\big(f(y)\big)$, c'est-à-dire $g \circ f(x + y) = g \circ f(x) + g \circ f(y)$. De plus, si $\lambda \in \mathbf{K}$, on a $g \circ f(\lambda x) = g\big(f(\lambda x)\big) = g\big(\lambda f(x)\big) = \lambda g\big(f(x)\big) = \lambda\big(g \circ f(x)\big)$. Ainsi, l'application $g \circ f$ est linéaire. ∎



## 2. Application linéaire et sous-espace vectoriel

Dans ce paragraphe, $E$, $F$ sont des $\mathbf{K}$-espaces vectoriels et $f$ est une application linéaire de $E$ dans $F$.

On rappelle que si $G$ est une partie de $E$, alors l'image de $G$ par $f$ est la partie $f(G)$ constituée des éléments de $F$ de la forme $f(x)$, où $x$ est un élément de $G$ (voir chapitre 2).

**Proposition.** *Si $G$ est un sous-espace vectoriel de $E$, alors $f(G)$ est un sous-espace vectoriel de $F$.*

**Démonstration.** Puisqu'on a $f(0)=0$ et puisque le vecteur nul de $E$ appartient à $G$, on en déduit que le vecteur nul de $F$ appartient à $f(G)$. Soient $y, y' \in f(G)$. Par définition de $f(G)$, il existe $x, x' \in G$ tels que $y = f(x)$ et $y' = f(x')$. Il vient $y + y' = f(x) + f(x')$, puis $y + y' = f(x + x')$, car l'application $f$ est linéaire. Mais $G$ est un sous-espace vectoriel de $E$, par suite $x + x' \in G$. On en déduit $y + y' \in f(G)$. De même on démontre que si $\lambda \in \mathbf{K}$, alors $\lambda y \in f(G)$. L'ensemble $f(G)$ est donc un sous-espace vectoriel de $F$. ∎

**Proposition.** *Si $G$ est le sous-espace vectoriel de $E$ engendré par les vecteurs $u_1, \ldots, u_n$, alors $f(G)$ est le sous-espace vectoriel de $F$ engendré par les vecteurs $f(u_1), \ldots, f(u_n)$.*

**Démonstration.** Puisque le vecteur $u_i$ appartient à $G$, il s'ensuit que $f(u_i)$ appartient à $f(G)$ pour tout $i$. Soit $y \in f(G)$. Il existe $x \in G$ tel que $y = f(x)$. Puisque $G$ est engendré par les vecteurs $u_1, \ldots, u_n$, il existe des scalaires $x_1, \ldots, x_n$ tels que $x = x_1 u_1 + \cdots + x_n u_n$. L'application $f$ étant linéaire, on en déduit $y = x_1 f(u_1) + \cdots + x_n f(u_n)$. Le sous-espace vectoriel $f(G)$ est donc engendré par les vecteurs $f(u_1), \ldots, f(u_n)$. ∎

**Définition**

On appelle *image* de $f$ le sous-espace vectoriel $f(E)$ de $F$ et on le note $\operatorname{Im} f$.

Si $E$ est de dimension $n \geqslant 1$ et si $(e_1, \ldots, e_n)$ est une base de $E$, alors la proposition précédente affirme que $\operatorname{Im} f$ est engendré par $f(e_1), \ldots, f(e_n)$. Il s'ensuit que si $E$ est de dimension finie, alors $\operatorname{Im} f$ est de dimension finie et l'on a $\dim \operatorname{Im} f \leqslant \dim E$.

**Proposition.** *L'ensemble des vecteurs $x$ de $E$ tels que $f(x) = 0$ est un sous-espace vectoriel de $E$. Ce sous-espace vectoriel s'appelle le noyau de $f$ et se note* $\operatorname{Ker} f$.

**Démonstration.** Puisque $f(0) = 0$, le vecteur nul de $E$ appartient à $\operatorname{Ker} f$. Si $\lambda$ est un scalaire et si $x$ et $y$ sont des vecteurs de $E$, on a $f(x + y) = f(x) + f(y)$ et $f(\lambda x) = \lambda f(x)$ car l'application $f$ est linéaire. Il s'ensuit que si $f(x) = 0$ et $f(y) = 0$,

alors $f(x+y)=0$ et $f(\lambda x)=0$. On a donc démontré que si $x$ et $y$ appartiennent à $\mathrm{Ker}\, f$, alors $x+y$ et $\lambda x$ aussi, d'où le résultat. ∎

**Proposition.** *L'application $f$ est injective si et seulement si l'on a $\mathrm{Ker}\, f = \{0\}$.*

**Démonstration.** Supposons l'application $f$ injective. Si $x$ est un vecteur de $\mathrm{Ker}\, f$, alors $f(x)=0$, donc $f(x)=f(0)$. Puisque l'application $f$ est injective, il s'ensuit $x=0$. Par conséquent on a $\mathrm{Ker}\, f = \{0\}$. Réciproquement, supposons que l'on a $\mathrm{Ker}\, f = \{0\}$. Soient $x$ et $y$ des vecteurs de $E$ tels que $f(x)=f(y)$. Il vient $f(x)-f(y)=0$. Mais l'application $f$ est linéaire, par suite on a $f(x-y)=0$, c'est-à-dire $x-y \in \mathrm{Ker}\, f$. Puisque $\mathrm{Ker}\, f = \{0\}$, il vient $x-y=0$, c'est-à-dire $x=y$. On a ainsi démontré que pour tous $x, y \in E$, si $f(x)=f(y)$, alors $x=y$. L'application $f$ est donc injective. ∎

Utilisez toujours cette proposition pour montrer qu'une application linéaire est injective.

**Théorème de la dimension.** *Supposons $E$ de dimension finie. Alors on a*

$$\dim E = \dim \mathrm{Ker}\, f + \dim \mathrm{Im}\, f.$$

**Démonstration.** Puisque $E$ est de dimension finie, le sous-espace vectoriel $\mathrm{Ker}\, f$ a un supplémentaire, d'après le corollaire page 120. Choisissons-en un, $S$. Alors on a $E = \mathrm{Ker}\, f + S$ et $S \cap \mathrm{Ker}\, f = \{0\}$. Soit $g : S \to \mathrm{Im}\, f$ l'application définie par $g(x) = f(x)$ pour tout $x \in S$. Puisque l'application $f$ est linéaire, l'application $g$ l'est également. Soit $x \in S$ tel que $g(x)=0$, c'est-à-dire tel que $f(x)=0$. On a donc $x \in S \cap \mathrm{Ker}\, f$ et par suite $x=0$. L'application $g$ est donc injective, d'après la proposition précédente. Soit $y \in \mathrm{Im}\, f$. Par définition de $\mathrm{Im}\, f$, il existe $x \in E$ tel que $y = f(x)$. Puisque $E = \mathrm{Ker}\, f + S$, on a $x = x_1 + x_2$, où $x_1 \in \mathrm{Ker}\, f$ et $x_2 \in S$. Il vient

$$y = f(x) = f(x_1+x_2) = f(x_1)+f(x_2) = 0 + f(x_2) = f(x_2) = g(x_2).$$

L'application $g$ est donc surjective. Il s'ensuit que $g$ est un isomorphisme de $S$ sur $\mathrm{Im}\, f$ et par suite $\dim S = \dim \mathrm{Im}\, f$. Enfin, puisque $E = \mathrm{Ker}\, f \oplus S$, nous savons que l'on a $\dim E = \dim \mathrm{Ker}\, f + \dim S$, d'où le résultat. ∎

**Corollaire.** *Supposons $E$ et $F$ de même dimension. Si l'application $f$ est injective ou si elle est surjective, alors $f$ est un isomorphisme.*

**Démonstration.** L'application $f$ est injective si et seulement si on a $\mathrm{Ker}\, f = \{0\}$, c'est-à-dire $\dim \mathrm{Ker}\, f = 0$. D'autre part, l'application $f$ est surjective si et seulement si on a $\mathrm{Im}\, f = F$, c'est-à-dire $\dim \mathrm{Im}\, f = \dim F$, ou encore $\dim \mathrm{Im}\, f = \dim E$. Grâce au théorème de la dimension, l'application $f$ est injective si et seulement si elle est surjective, d'où le résultat. ∎





Appliquons le théorème de la dimension en supposant $E$ de dimension $n \geqslant 1$ et $F = \mathbf{K}$. Si $f$ est une forme linéaire non nulle sur $E$, on a $\mathrm{Im}\, f \neq \{0\}$, donc $\dim \mathrm{Im}\, f \geqslant 1$. D'autre part, on a $\mathrm{Im}\, f \subset \mathbf{K}$, par suite $\dim \mathrm{Im}\, f \leqslant 1$. Il s'ensuit $\dim \mathrm{Im}\, f = 1$ et par suite $\dim \mathrm{Ker}\, f = n-1$.

Soient $n$ un entier supérieur ou égal à 2 et $a_1, a_2, \ldots, a_n \in \mathbf{K}$ des scalaires non tous nuls. Alors le sous-espace vectoriel de $\mathbf{K}^n$ d'équation $a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0$ est de dimension $n-1$.

## 3. Matrice d'une application linéaire

Dans ce paragraphe, $E$ et $E'$ sont des $\mathbf{K}$-espaces vectoriels différents de $\{0\}$ et de dimension finie. Posons $p = \dim E$, $n = \dim E'$ et considérons $(e_1, \ldots, e_p)$ une base de $E$ et $(e'_1, \ldots, e'_n)$ une base de $E'$.

**Définitions**

Soit $f$ une application linéaire de $E$ dans $E'$. La *matrice de $f$ dans les bases $(e_1,\ldots,e_p)$ et $(e'_1,\ldots,e'_n)$* est la matrice appartenant à $M_{n,p}(\mathbf{K})$, dont les coefficients de la $j$-ième colonne sont les coordonnées du vecteur $f(e_j)$ dans la base $(e'_1,\ldots,e'_n)$.

Si $E' = E$ et $e'_i = e_i$ pour tout $i$, alors la matrice de $f$ dans les bases $(e_1,\ldots,e_p)$ et $(e_1,\ldots,e_p)$ s'appelle plus simplement *la matrice de $f$ dans la base $(e_1,\ldots,e_p)$*.

Supposons $p = 4$, $n = 3$ et supposons que $f$ est l'unique application linéaire de $E$ dans $E'$ telle que

$$\begin{cases} f(e_1) = e'_1 - 2e'_2 + 6e'_3 \\ f(e_2) = 3e'_1 + e'_3 \\ f(e_3) = e'_2 - e'_3 \\ f(e_4) = e'_1 + e'_2 + e'_3. \end{cases}$$

Alors la matrice de $f$ dans les bases $(e_1, e_2, e_3, e_4)$ et $(e'_1, e'_2, e'_3)$ est la matrice

$$\begin{bmatrix} 1 & 3 & 0 & 1 \\ -2 & 0 & 1 & 1 \\ 6 & 1 & -1 & 1 \end{bmatrix}.$$

### Exemples

- La matrice de $\mathrm{id}_E$ dans n'importe quelle base de $E$ est $I_p$. Rappelons que $I_p$ est la matrice diagonale dont tous les coefficients diagonaux sont égaux à 1.
- Soit $f : \mathbf{R}^2 \to \mathbf{R}^3$ l'application linéaire définie par $f(x,y) = (x+y, -x+2y, y)$ pour tous $x, y \in \mathbf{R}$. On a $f(1,0) = (1,-1,0)$ et $f(0,1) = (1,2,1)$, par suite la matrice de $f$ dans les bases canoniques de $\mathbf{R}^2$ et $\mathbf{R}^3$ est

$$\begin{bmatrix} 1 & 1 \\ -1 & 2 \\ 0 & 1 \end{bmatrix}.$$

La proposition suivante résulte immédiatement des définitions de la somme et de la multiplication par un scalaire des applications linéaires et des matrices.

**Proposition.** *Soient $f$ et $g$ des applications linéaires de $E$ dans $E'$ et soit $\lambda \in \mathbf{K}$. Si $A$ est la matrice de $f$ et si $B$ est la matrice de $g$ dans les bases $(e_1, \ldots, e_p)$ et $(e'_1, \ldots, e'_n)$, alors la matrice de $f+g$ dans ces bases est $A+B$ et la matrice de $\lambda f$ est $\lambda A$.*

Grâce à la proposition qui suit, nous allons voir que la matrice d'une application linéaire $f$ permet de calculer les coordonnées de $f(x)$ lorsqu'on connaît celles de $x$.

**Proposition.** *Soit $f$ une application linéaire de $E$ dans $E'$ et soit $A$ la matrice de $f$ dans les bases $(e_1, \ldots, e_p)$ et $(e'_1, \ldots, e'_n)$. Si $x$ est un vecteur de $E$ et si l'on note*

$$X = \begin{bmatrix} x_1 \\ \vdots \\ x_p \end{bmatrix} \quad et \quad Y = \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix},$$

*où $x_1, \ldots, x_p$ sont les coordonnées de $x$ dans la base $(e_1, \ldots, e_p)$ et où $y_1, \ldots, y_n$ sont les coordonnées de $f(x)$ dans la base $(e'_1, \ldots, e'_n)$, alors on a $Y = AX$.*

**Démonstration.** On a $f(x) = x_1 f(e_1) + \cdots + x_p f(e_p)$ car l'application $f$ est linéaire. Si $A$ est la matrice $[a_{ij}]$, alors par définition de $A$, on a

$$\begin{cases} f(e_1) = a_{11}e'_1 + \cdots + a_{n1}e'_n \\ \vdots \qquad\qquad\qquad \vdots \\ f(e_p) = a_{1p}e'_1 + \cdots + a_{np}e'_n \end{cases}$$

et donc $f(x) = (a_{11}x_1 + \cdots + a_{1p}x_p)e'_1 + \cdots + (a_{n1}x_1 + \cdots + a_{np}x_p)e'_n$. Par unicité des coordonnées de $f(x)$ dans la base $(e'_1, \ldots, e'_n)$, on a donc

$$\begin{cases} y_1 = a_{11}x_1 + \cdots + a_{1p}x_p \\ \vdots \qquad\qquad\qquad \vdots \\ y_n = a_{n1}x_1 + \cdots + a_{np}x_p \end{cases}$$

ce qui se traduit matriciellement par $Y = AX$. ∎





**Exemple.** Soit $(\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3)$ la base canonique de $\mathbf{R}^3$ et soit $f : \mathbf{R}^3 \to \mathbf{R}^3$ l'unique application linéaire telle que

$$\begin{cases} f(\mathbf{e}_1) = \mathbf{e}_1 - \mathbf{e}_2 + 2\mathbf{e}_3 \\ f(\mathbf{e}_2) = 2\mathbf{e}_1 + 3\mathbf{e}_3 \\ f(\mathbf{e}_3) = \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3. \end{cases}$$

La matrice de $f$ dans la base $(\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3)$ est

$$\begin{bmatrix} 1 & 2 & 1 \\ -1 & 0 & 1 \\ 2 & 3 & 1 \end{bmatrix}$$

et pour tous nombres réels $x, y, z$, on a

$$\begin{bmatrix} 1 & 2 & 1 \\ -1 & 0 & 1 \\ 2 & 3 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} x+2y+z \\ -x+z \\ 2x+3y+z \end{bmatrix}.$$

On a donc $f(x,y,z) = (x+2y+z, -x+z, 2x+3y+z)$ pour tous $x, y, z \in \mathbf{R}$.

Dans la proposition suivante, $E''$ est un $\mathbf{K}$-espace vectoriel de dimension $q \geqslant 1$ et $(e''_1, \ldots, e''_q)$ est une base de $E''$. Dans cette proposition, nous allons voir que le produit matriciel correspond à la composée des applications linéaires.

**Proposition.** *Soit $f$ une application linéaire de $E$ dans $E'$ et soit $g$ une application linéaire de $E'$ dans $E''$. Si $A$ est la matrice de $f$ dans les bases $(e_1, \ldots, e_p)$ et $(e'_1, \ldots, e'_n)$ et si $B$ est la matrice de $g$ dans les bases $(e'_1, \ldots, e'_n)$ et $(e''_1, \ldots, e''_q)$, alors la matrice de $g \circ f$ dans les bases $(e_1, \ldots, e_p)$ et $(e''_1, \ldots, e''_q)$ est la matrice $BA$.*

**Démonstration.** Soit $x$ un vecteur de $E$. Notons $x_1, \ldots, x_p$ les coordonnées de $x$ dans la base $(e_1, \ldots, e_p)$, $y_1, \ldots, y_n$ celles de $f(x)$ dans la base $(e'_1, \ldots, e'_n)$ et $z_1, \ldots, z_q$ celles de $g \circ f(x)$ dans la base $(e''_1, \ldots, e''_q)$. Notons $X$, $Y$ et $Z$ les matrices-colonnes correspondantes, de sorte que l'on a $Y = AX$ et $Z = BY$. D'après les règles du calcul matriciel, il vient $Z = B(AX) = (BA)X$. Appliquons ce résultat lorsque $x$ est le vecteur $e_j$ : la $j$-ième colonne de la matrice de $g \circ f$ dans les bases $(e_1, \ldots, e_p)$ et $(e''_1, \ldots, e''_q)$ est la $j$-ième colonne de la matrice $BA$. La matrice de $g \circ f$ dans les bases $(e_1, \ldots, e_p)$ et $(e''_1, \ldots, e''_q)$ est donc $BA$. ∎

Voici comment reconnaître un isomorphisme au moyen de sa matrice.

**Proposition.** *Supposons que les espaces vectoriels $E$ et $E'$ ont la même dimension $p$. Soit $f$ une application linéaire de $E$ dans $E'$ et soit $A$ la matrice de $f$ dans les bases $(e_1, \ldots, e_p)$ et $(e'_1, \ldots, e'_p)$. L'application $f$ est un isomorphisme si et seulement si la matrice $A$ est inversible. De plus, si $f$ est un isomorphisme, alors la matrice de $f^{-1}$ dans les bases $(e'_1, \ldots, e'_p)$ et $(e_1, \ldots, e_p)$ est $A^{-1}$.*

**Démonstration.** Nous savons que $f$ est un isomorphisme si et seulement si $(f(e_1), \ldots, f(e_p))$ est une base de $E'$. La matrice $A$ est celle des coordonnées de $f(e_1), \ldots, f(e_p)$ dans la base $(e'_1, \ldots, e'_p)$. Or d'après le corollaire page 115, les vecteurs $f(e_1), \ldots, f(e_p)$ forment une base de $E'$ si et seulement si la matrice $A$ est inversible. Si $f$ est un isomorphisme, notons $B$ la matrice de $f^{-1}$ dans les bases $(e'_1, \ldots, e'_p)$ et $(e_1, \ldots, e_p)$. D'après la proposition précédente, la matrice de $f^{-1} \circ f$ dans la base $(e_1, \ldots, e_p)$ est la matrice $BA$. Mais on a $f^{-1} \circ f = \mathrm{id}_E$, par suite la matrice de $f^{-1} \circ f$ dans la base $(e_1, \ldots, e_p)$ est $I_p$. Il s'ensuit $BA = I_p$ et donc $B = A^{-1}$. ∎

Terminons ce paragraphe par des résultats concernant des applications linéaires particulièrement importantes, celles de $E$ dans $E$.

### Changement de base

Supposons que $(u_1, \ldots, u_p)$ et $(u'_1, \ldots, u'_p)$ sont des bases de $E$.

**Définition**

La matrice $P$ de $M_p(\mathbf{K})$ dont les coefficients de la $j$-ième colonne sont les coordonnées du vecteur $u'_j$ dans la base $(u_1, \ldots, u_p)$ s'appelle la *matrice de passage* de la base $(u_1, \ldots, u_p)$ à la base $(u'_1, \ldots, u'_p)$.

L'application identique de $E$ vérifie $\mathrm{id}_E(u'_j) = u'_j$ pour tout $j$. Par définition de la matrice d'une application linéaire, la matrice de $\mathrm{id}_E$ dans les bases $(u'_1, \ldots, u'_p)$ et $(u_1, \ldots, u_p)$ est donc $P$. D'après la proposition précédente, il s'ensuit qu'une matrice de passage est toujours inversible, car $\mathrm{id}_E$ est un isomorphisme de $E$ sur $E$.

Soit $x$ un vecteur de $E$. Notons $X = \begin{bmatrix} x_1 \\ \vdots \\ x_p \end{bmatrix}$ les coordonnées de $x$ dans la base $(u_1, \ldots, u_p)$ et $X' = \begin{bmatrix} x'_1 \\ \vdots \\ x'_p \end{bmatrix}$ les coordonnées de $x$ dans la base $(u'_1, \ldots, u'_p)$. D'après une proposition page 142, l'égalité vectorielle $x = \mathrm{id}_E(x)$ se traduit par la relation matricielle $X = PX'$.





Dans la pratique, le vecteur $x$ et les vecteurs $u'_1, \ldots, u'_p$ sont définis par leurs coordonnées dans la base $(u_1, \ldots, u_p)$, autrement dit on connaît la matrice de passage $P$ et la matrice-colonne $X$. Pour trouver les coordonnées de $x$ dans la base $(u'_1, \ldots, u'_p)$, on est alors conduit à calculer la matrice $P^{-1}$ et l'on aura $X' = P^{-1}X$. Les calculs à faire sont ceux que nous avons pratiqués pour le changement de coordonnées page 116.

Étudions maintenant l'effet d'un changement de base sur la matrice d'une application linéaire de $E$ dans $E$.

**Théorème.** *Supposons que $(u_1, \ldots, u_p)$ et $(u'_1, \ldots, u'_p)$ sont des bases de $E$. Soient $f$ une application linéaire de $E$ dans $E$, $A$ la matrice de $f$ dans la base $(u_1, \ldots, u_p)$ et $A'$ la matrice de $f$ dans la base $(u'_1, \ldots, u'_p)$. Si $P$ est la matrice de passage de la base $(u_1, \ldots, u_p)$ à la base $(u'_1, \ldots, u'_p)$, alors on a $A' = P^{-1}AP$.*

**Démonstration.** Nous avons déjà remarqué que $P$ est la matrice de $\mathrm{id}_E$ dans les bases $(u'_1, \ldots, u'_p)$ et $(u_1, \ldots, u_p)$. En appliquant une proposition précédente, la matrice de $f \circ \mathrm{id}_E$ dans les bases $(u'_1, \ldots, u'_p)$ et $(u_1, \ldots, u_p)$ est $AP$ et la matrice de $\mathrm{id}_E \circ f$ dans ces mêmes bases est $PA'$. Puisqu'on a $f \circ \mathrm{id}_E = \mathrm{id}_E \circ f$, il vient $AP = PA'$. On en déduit $A' = P^{-1}AP$. ∎

L'égalité $A' = P^{-1}AP$ s'appelle la *formule de changement de base*.

La formule de changement de base a un grand intérêt théorique, mais pratiquement, on ne l'emploie pas pour calculer $A'$ à partir de $P$ et $A$.

**Exercice 1.** Soit $(\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3)$ la base canonique de $\mathbf{R}^3$ et soit $f : \mathbf{R}^3 \to \mathbf{R}^3$ l'application linéaire définie par $f(x, y, z) = (-x + y + z, -2x + y + z, -6x + 2y + 4z)$ pour tous $x, y, z \in \mathbf{R}$. Notons $A$ la matrice de $f$ dans la base $(\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3)$.

a) Écrire la matrice $A$.

b) Considérons les vecteurs de $\mathbf{R}^3$ : $v_1 = (1, 0, 2)$, $v_2 = (1, 1, 2)$ et $v_3 = (2, 1, 5)$. Montrer que $(v_1, v_2, v_3)$ est une base de $\mathbf{R}^3$ et calculer la matrice de $f$ dans cette base.

**Réponse**

a) On a $f(\mathbf{e}_1) = f(1, 0, 0) = (-1, -2, -6)$, $f(\mathbf{e}_2) = f(0, 1, 0) = (1, 1, 2)$ et $f(\mathbf{e}_3) = f(0, 0, 1) = (1, 1, 4)$. Il s'ensuit

$$A = \begin{bmatrix} -1 & 1 & 1 \\ -2 & 1 & 1 \\ -6 & 2 & 4 \end{bmatrix}.$$

**b)** Soit $P$ la matrice de $M_3(\mathbf{R})$ dont les colonnes sont les coordonnées des vecteurs $v_1$, $v_2$ et $v_3$ dans la base $(\mathrm{e}_1, \mathrm{e}_2, \mathrm{e}_3)$. Il vient

$$P = \begin{bmatrix} 1 & 1 & 2 \\ 0 & 1 & 1 \\ 2 & 2 & 5 \end{bmatrix} \quad \text{et} \quad \det P = \begin{vmatrix} 1 & 1 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{vmatrix} = \begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix} = 1.$$

La matrice $P$ est donc inversible, par suite $(v_1, v_2, v_3)$ est une base de $\mathbf{R}^3$. On a $f(v_1) = f(1,0,2) = (1,0,2)$, $f(v_2) = f(1,1,2) = (2,1,4)$ et $f(v_3) = f(2,1,5) = (4,2,10)$. On en déduit $f(v_1) = v_1$ et $f(v_3) = 2v_3$. Les coordonnées de $f(v_2)$ dans la base $(v_1, v_2, v_3)$ sont les nombres réels $a, b, c$ tels que $f(v_2) = av_1 + bv_2 + cv_3$, c'est-à-dire les solutions des systèmes d'équations linéaires équivalents suivants :

$$\begin{cases} a + b + 2c = 2 \\ b + c = 1 \\ 2a + 2b + 5c = 4 \end{cases} \iff \begin{cases} a + b + 2c = 2 \\ b + c = 1 \\ c = 0 \end{cases} \iff \begin{cases} a = 1 \\ b = 1 \\ c = 0. \end{cases}$$

Il s'ensuit $f(v_2) = v_1 + v_2$. On a ainsi $\begin{cases} f(v_1) = v_1 \\ f(v_2) = v_1 + v_2 \\ f(v_3) = 2v_3 \end{cases}$. La matrice de $f$ dans la base $(v_1, v_2, v_3)$ est donc

$$B = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix}.$$

D'après la formule de changement de base, nous savons que l'on a l'égalité matricielle $B = P^{-1}AP$.

> **Pour calculer la matrice d'une application linéaire dans une base, revenez toujours à la définition.**

Terminons ce chapitre par deux exercices où l'on utilise plusieurs résultats d'algèbre linéaire et où nous posons des questions auxquelles il est indispensable de savoir répondre.

**Exercice 2.** Soient $E$ un $\mathbf{R}$-espace vectoriel de dimension 3 et $(e_1, e_2, e_3)$ une base de $E$. Soit $f : E \to E$ l'application linéaire dont la matrice dans la base $(e_1, e_2, e_3)$ est

$$\begin{bmatrix} 1 & 1 & -1 \\ 4 & 1 & -2 \\ 6 & 3 & -4 \end{bmatrix}.$$

**a)** Trouver une base de $\operatorname{Ker} f$.

**b)** Posons $v_1 = e_1 + 2e_2 + 3e_3$, $v_2 = e_2 + e_3$ et $v_3 = e_1 + 2e_3$. Montrer que $(v_1, v_2, v_3)$ est une base de $E$. Calculer la matrice de $f$ dans la base $(v_1, v_2, v_3)$.

**c)** En déduire que l'on a $f \circ f = -f$.



**Réponse**

**a)** Le vecteur $xe_1 + ye_2 + ze_3$ appartient à $\operatorname{Ker} f$ si et seulement si on a

$$\begin{bmatrix} 1 & 1 & -1 \\ 4 & 1 & -2 \\ 6 & 3 & -4 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = 0.$$

Résolvons ce système d'équations linéaires. Il vient

$$xe_1 + ye_2 + ze_3 \in \operatorname{Ker} f \iff \begin{cases} x + y - z = 0 \\ 4x + y - 2z = 0 \\ 6x + 3y - 4z = 0 \end{cases} \iff \begin{cases} x + y - z = 0 \\ -3y + 2z = 0 \end{cases}$$
$$\iff (x, y, z) = x(1, 2, 3)$$
$$\iff xe_1 + ye_2 + ze_3 = x(e_1 + 2e_2 + 3e_3).$$

Une base de $\operatorname{Ker} f$ est donc $e_1 + 2e_2 + 3e_3$.

**b)** Soit $P$ la matrice dont les colonnes sont les coordonnées de $v_1, v_2, v_3$ dans la base $(e_1, e_2, e_3)$. On a

$$P = \begin{bmatrix} 1 & 0 & 1 \\ 2 & 1 & 0 \\ 3 & 1 & 2 \end{bmatrix} \quad \text{et} \quad \det P = \begin{vmatrix} 1 & 0 & 1 \\ 2 & 1 & 0 \\ 3 & 1 & 2 \end{vmatrix} = \begin{vmatrix} 0 & 0 & 1 \\ 2 & 1 & 0 \\ 1 & 1 & 2 \end{vmatrix} = \begin{vmatrix} 2 & 1 \\ 1 & 1 \end{vmatrix} = 1.$$

Puisque la matrice $P$ est inversible, les vecteurs $v_1, v_2, v_3$ forment une base de $E$. D'après la question précédente, il vient $f(v_1) = 0$. D'autre part on a

$$f(v_2) = f(e_2) + f(e_3) = (e_1 + e_2 + 3e_3) + (-e_1 - 2e_2 - 4e_3) = -e_2 - e_3 = -v_2$$
$$f(v_3) = f(e_1) + 2f(e_3) = (e_1 + 4e_2 + 6e_3) + 2(-e_1 - 2e_2 - 4e_3)$$
$$= -e_1 - 2e_3 = -v_3.$$

La matrice de $f$ dans la base $(v_1, v_2, v_3)$ est donc

$$M = \begin{bmatrix} 0 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}.$$

**c)** La matrice de $f \circ f$ dans la base $(v_1, v_2, v_3)$ est $M^2 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$. On a donc $M^2 = -M$.

Puisque $-M$ est la matrice de $-f$ dans la base $(v_1, v_2, v_3)$, il s'ensuit $f \circ f = -f$.

**Exercice 3.** Notons $(\mathrm{e}_1, \mathrm{e}_2, \mathrm{e}_3)$ la base canonique de $\mathbf{R}^3$. Soit $f : \mathbf{R}^3 \to \mathbf{R}^3$ l'unique application linéaire telle que

$$\begin{cases} f(\mathrm{e}_1) = -\mathrm{e}_1 + \mathrm{e}_2 + \mathrm{e}_3 \\ f(\mathrm{e}_2) = -2\mathrm{e}_1 + 2\mathrm{e}_3 \\ f(\mathrm{e}_3) = -4\mathrm{e}_1 + \mathrm{e}_2 + 4\mathrm{e}_3. \end{cases}$$

Notons $A$ la matrice de $f$ dans la base $(\mathrm{e}_1, \mathrm{e}_2, \mathrm{e}_3)$.

**a)** Écrire la matrice $A$.

**b)** Donner une base de $\operatorname{Im} f$ et une équation de $\operatorname{Im} f$.

c) Pour quelles valeurs du nombre réel $t$ l'application linéaire $f - t\,\mathrm{id}_{\mathbb{R}^3}$ est-elle un isomorphisme ?

d) Trouver une base $v_1$ de $\operatorname{Ker}(f - 3\,\mathrm{id}_{\mathbb{R}^3})$ et une base $v_2$ de $\operatorname{Ker} f$. Montrer que les vecteurs $v_1$ et $v_2$ sont linéairement indépendants. Trouver $v_3 \in \mathbb{R}^3$ tel que $(v_1, v_2, v_3)$ est une base de $\mathbb{R}^3$. Quelle est la matrice de $f$ dans la base $(v_1, v_2, v_3)$ ?

**Réponse**

a) Par définition de la matrice de $f$ dans une base de $\mathbb{R}^3$, il vient

$$A = \begin{bmatrix} -1 & -2 & -4 \\ 1 & 0 & 1 \\ 1 & 2 & 4 \end{bmatrix}.$$

b) Le sous-espace vectoriel $\operatorname{Im} f$ est engendré par $f(\mathbf{e}_1)$, $f(\mathbf{e}_2)$ et $f(\mathbf{e}_3)$. Pratiquons la méthode de Gauss sur les colonnes de la matrice $A$ pour trouver une base de $\operatorname{Im} f$. On obtient successivement les matrices

$$\begin{bmatrix} -1 & 0 & 0 \\ 1 & -2 & -3 \\ 1 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} -1 & 0 & 0 \\ 1 & 1 & -3 \\ 1 & 0 & 0 \end{bmatrix} \quad \text{et} \quad \begin{bmatrix} -1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

Les vecteurs $(-1, 1, 1) = -\mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3$ et $(0, 1, 0) = \mathbf{e}_2$ forment donc une base de $\operatorname{Im} f$. De plus, le vecteur $(x, y, z)$ de $\mathbb{R}^3$ appartient à $\operatorname{Im} f$ si et seulement si on a

$$\begin{vmatrix} -1 & 0 & x \\ 1 & 1 & y \\ 1 & 0 & z \end{vmatrix} = 0, \quad \text{soit} \quad x \begin{vmatrix} 1 & 1 \\ 1 & 0 \end{vmatrix} - y \begin{vmatrix} -1 & 0 \\ 1 & 0 \end{vmatrix} + z \begin{vmatrix} -1 & 0 \\ 1 & 1 \end{vmatrix} = 0.$$

Une équation de $\operatorname{Im} f$ est donc $x + z = 0$.

c) Soit $t \in \mathbb{R}$. L'application linéaire $f - t\,\mathrm{id}_{\mathbb{R}^3}$ est un isomorphisme si et seulement si sa matrice dans la base $(\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3)$ est inversible. Or la matrice de $f - t\,\mathrm{id}_{\mathbb{R}^3}$ dans cette base est $A - tI_3$ et le déterminant de cette matrice est

$$\begin{vmatrix} -1-t & -2 & -4 \\ 1 & -t & 1 \\ 1 & 2 & 4-t \end{vmatrix} = \begin{vmatrix} -t & 0 & -t \\ 1 & -t & 1 \\ 1 & 2 & 4-t \end{vmatrix} = \begin{vmatrix} -t & 0 & 0 \\ 1 & -t & 0 \\ 1 & 2 & 3-t \end{vmatrix} = t^2(3-t).$$

Il s'ensuit que l'application linéaire $f - t\,\mathrm{id}_{\mathbb{R}^3}$ est un isomorphisme si et seulement si $t \neq 0$ et $t \neq 3$.

d) Soit $u = (x, y, z)$ un vecteur de $\mathbb{R}^3$. La matrice de $f - 3\,\mathrm{id}_{\mathbb{R}^3}$ dans la base $(\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3)$ est $A - 3I_3$. En utilisant le calcul matriciel, on a les équivalences

$$u \in \operatorname{Ker}(f - 3\,\mathrm{id}_{\mathbb{R}^3}) \Longleftrightarrow (A - 3I_3) \begin{bmatrix} x \\ y \\ z \end{bmatrix} = 0 \Longleftrightarrow \begin{cases} -4x - 2y - 4z = 0 \\ x - 3y + z = 0 \\ x + 2y + z = 0 \end{cases}$$

$$\Longleftrightarrow \begin{cases} x + 2y + z = 0 \\ 6y = 0 \\ -5y = 0 \end{cases} \Longleftrightarrow \begin{cases} x + z = 0 \\ y = 0 \end{cases} \Longleftrightarrow \begin{bmatrix} x \\ y \\ z \end{bmatrix} = x \begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix}.$$

Une base de $\operatorname{Ker}(f - 3\mathrm{id}_{\mathbb{R}^3})$ est donc le vecteur $v_1 = (1, 0, -1) = \mathbf{e}_1 - \mathbf{e}_3$. De même on a





$$u \in \operatorname{Ker} f \Longleftrightarrow A \begin{bmatrix} x \\ y \\ z \end{bmatrix} = 0 \Longleftrightarrow \begin{cases} -x - 2y - 4z = 0 \\ x + z = 0 \\ x + 2y + 4z = 0 \end{cases}$$

$$\Longleftrightarrow \begin{cases} x + z = 0 \\ 2y + 3z = 0 \end{cases} \Longleftrightarrow \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \frac{y}{3} \begin{bmatrix} 2 \\ 3 \\ -2 \end{bmatrix}.$$

Une base de $\operatorname{Ker} f$ est donc le vecteur $v_2 = (2, 3, -2) = 2\mathbf{e}_1 + 3\mathbf{e}_2 - 2\mathbf{e}_3$. Le vecteur $v_1$ n'est pas nul. Puisque la deuxième coordonnée de $v_1$ dans la base $(\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3)$ est nulle alors que celle de $v_2$ n'est pas nulle, $v_2$ n'est pas colinéaire à $v_1$. Il s'ensuit que les vecteurs $v_1$ et $v_2$ sont linéairement indépendants. D'après le théorème de la base incomplète, nous savons qu'il existe un vecteur $\mathbf{e}_i$ tel que $(v_1, v_2, \mathbf{e}_i)$ est une base de $\mathbb{R}^3$. Puisque

$$\begin{vmatrix} 1 & 2 & 1 \\ 0 & 3 & 0 \\ -1 & -2 & 0 \end{vmatrix} = \begin{vmatrix} 0 & 3 \\ -1 & -2 \end{vmatrix} = 3,$$

il s'ensuit que $(v_1, v_2, \mathbf{e}_1)$ est une base de $\mathbb{R}^3$. Calculons la matrice de $f$ dans cette base. Puisque $v_1 \in \operatorname{Ker}(f - 3\,\mathrm{id}_{\mathbb{R}^3})$, on a $(f - 3\,\mathrm{id}_{\mathbb{R}^3})(v_1) = 0$, c'est-à-dire $f(v_1) - 3\,\mathrm{id}_{\mathbb{R}^3}(v_1) = f(v_1) - 3v_1 = 0$, ou encore $f(v_1) = 3v_1$. Il vient $f(v_2) = 0$ car $v_2 \in \operatorname{Ker} f$. Enfin, on a $f(\mathbf{e}_1) = -\mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3$, $\mathbf{e}_3 = \mathbf{e}_1 - v_1$ et $3\mathbf{e}_2 = -2v_1 + v_2$. Il s'ensuit $f(\mathbf{e}_1) = \frac{1}{3}(-5v_1 + v_2)$. La matrice de $f$ dans la base $(v_1, v_2, \mathbf{e}_1)$ est donc

$$\begin{bmatrix} 3 & 0 & -5/3 \\ 0 & 0 & 1/3 \\ 0 & 0 & 0 \end{bmatrix}.$$

## Exercices

1. Considérons les vecteurs de $\mathbb{R}^2$ : $u = (1, 1)$, $v = (2, -1)$ et $w = (1, 4)$.

   a) Montrer que $(u, v)$ est une base de $\mathbb{R}^2$.

   b) Pour quelles valeurs du nombre réel $a$ existe-il une application linéaire $f$ de $\mathbb{R}^2$ dans $\mathbb{R}^2$ telle que $f(u) = (2, 1)$, $f(v) = (1, -1)$ et $f(w) = (5, a)$ ?

2. Trouver une infinité d'isomorphismes $f$ de $\mathbb{R}^2$ vers $\mathbb{R}^2$ tels que $f(1, 1) = (1, 2)$.

3. Trouver toutes les formes linéaires $f$ sur $\mathbb{R}^3$ telles que $f(1, -1, 2) = 1$.

4. On considère les vecteurs de $\mathbb{R}^3$ : $u = (1, 2, 1)$, $v = (-1, 1, 1)$ et $w = (3, 0, -1)$.

   a) Montrer que $u$ et $v$ sont linéairement indépendants et que $w$ est combinaison linéaire de $u$ et $v$.

   b) Pour quelles valeurs du nombre réel $a$ existe-il une application linéaire $f$ de $\mathbb{R}^3$ dans $\mathbb{R}^3$ telle que $f(u) = (1, 1, 0)$, $f(v) = (0, 1, 1)$ et $f(w) = (1, -1, a)$ ?

**5.** Soient $E$ et $F$ des $\mathbf{K}$-espaces vectoriels. Soit $f$ une application linéaire de $E$ dans $F$. Soit $g : E \times F \to E \times F$ l'application définie par $g(x,y) = (x, y - f(x))$ pour tout $(x,y) \in E \times F$.

**a)** Montrer que $g$ est une application linéaire.

**b)** Montrer que $g$ est un isomorphisme.

**6.** Soient $E$ un $\mathbf{K}$-espace vectoriel de dimension 3 et $(e_1, e_2, e_3)$ une base de $E$. Soit $f$ l'application linéaire de $E$ dans $E$ dont la matrice dans la base $(e_1, e_2, e_3)$ est

$$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 2 & 1 \\ 2 & -1 & 2 \end{bmatrix}.$$

**a)** Écrire la matrice de $f$ dans la base $(e_3, e_2, e_1)$.

**b)** Écrire la matrice de $f$ dans la base $(e_1 + e_3, e_3, e_2 - e_3)$.

**7.** Soit $f$ l'application linéaire de $\mathbf{R}^2$ dans $\mathbf{R}^2$ dont la matrice dans la base canonique est

$$\begin{bmatrix} 4 & 4 \\ -1 & 0 \end{bmatrix}.$$

**a)** Trouver des vecteurs $u$ et $v$ de $\mathbf{R}^2$ tels que $u \neq 0$, $f(u) = 2u$ et $f(v) = u + 2v$.

**b)** Soient $u$ et $v$ des vecteurs de $\mathbf{R}^2$ tels que $u \neq 0$, $f(u) = 2u$ et $f(v) = u + 2v$. Montrer que $(u, v)$ est une base de $\mathbf{R}^2$. Écrire la matrice de $f$ dans cette base.

**8.** Soit $D_1$ la droite de $\mathbf{R}^2$ d'équation $x + y = 0$ et soit $D_2$ la droite de $\mathbf{R}^2$ d'équation $3x + y = 0$. Notons $s$ la symétrie de $\mathbf{R}^2$ par rapport à $D_1$ parallèlement à $D_2$.

**a)** Quelle est la matrice de $s$ dans la base canonique de $\mathbf{R}^2$ ?

**b)** Calculer $s \circ s$. En déduire que $s$ est une application bijective.

**c)** Soit $D$ une droite de $\mathbf{R}^2$. Montrer que $s(D)$ est une droite de $\mathbf{R}^2$.

**d)** Soit $D$ la droite de $\mathbf{R}^2$ d'équation $2x - y = 0$. Trouver une équation de $s(D)$.

**9.** Soit $P$ le sous-espace vectoriel de $\mathbf{R}^3$ d'équation $x + 2y - z = 0$ et soit $D$ le sous-espace vectoriel de $\mathbf{R}^3$ d'équations $\begin{cases} x + y = 0 \\ y + z = 0 \end{cases}$.

**a)** Montrer que $P$ et $D$ sont supplémentaires. Trouver une base de $P$ et une base de $D$.

**b)** Notons $p$ la projection de $\mathbf{R}^3$ sur $P$ parallèlement à $D$ et $s$ la symétrie de $\mathbf{R}^3$ par rapport à $P$ parallèlement à $D$. Calculer les matrices de $p$ et de $s$ dans la base canonique de $\mathbf{R}^3$.





**10. a)** On considère la matrice suivante de $M_2(\mathbf{R})$ :

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Calculer $A^2$ et $(P^{-1}AP)^2$ pour toute matrice inversible $P$ de $M_2(\mathbf{R})$.

**b)** Trouver explicitement une infinité d'applications linéaires $f$ de $\mathbf{R}^2$ dans $\mathbf{R}^2$ telles que $f \circ f = -\mathrm{id}_{\mathbf{R}^2}$.

**c)** Soit $f$ une application linéaire de $\mathbf{R}^2$ dans $\mathbf{R}^2$ telle que $f \circ f = -\mathrm{id}_{\mathbf{R}^2}$. Montrer que $f$ est un isomorphisme.

**11.** Soient $E$ un $\mathbf{R}$-espace vectoriel de dimension 2 et $f$ une application linéaire de $E$ dans $E$ telle que $f \circ f = -\mathrm{id}_E$.

**a)** Soit $x$ un vecteur non nul de $E$. Montrer que $(x, f(x))$ est une base de $E$.

**b)** Soit $x$ un vecteur non nul de $E$. Écrire la matrice de $f$ dans la base $(x, f(x))$.

**12.** Soient $E$ un $\mathbf{R}$-espace vectoriel de dimension 4 et $f$ une application linéaire de $E$ dans $E$ telle que $f \circ f = -\mathrm{id}_E$.

**a)** Soit $x$ un vecteur non nul de $E$. Montrer que les vecteurs $x$ et $f(x)$ sont linéairement indépendants.

**b)** Soit $x$ un vecteur non nul de $E$. Montrer qu'il existe $y \in E$ tel que les vecteurs $x$, $f(x)$ et $y$ sont linéairement indépendants. Montrer ensuite que $(x, f(x), y, f(y))$ est une base de $E$.

**c)** Soient $x, y \in E$ tels que $(x, f(x), y, f(y))$ est une base de $E$. Écrire la matrice de $f$ dans cette base.

**d)** Trouver une application linéaire $g$ de $\mathbf{R}^4$ dans $\mathbf{R}^4$ telle que $g \circ g = -\mathrm{id}_{\mathbf{R}^4}$.

**13.** Soit $m$ un nombre réel.

**a)** Calculer le déterminant de la matrice

$$\begin{bmatrix} 1 & -1 & m-2 \\ 2 & m-4 & -2 \\ m+2 & -4 & -3 \end{bmatrix}.$$

**b)** Soient $a, b, c$ des nombres réels. Résoudre le système d'équations linéaires

$$\begin{cases} x - y + (m-2)z = a \\ 2x + (m-4)y - 2z = b \\ (m+2)x - 4y - 3z = c. \end{cases}$$

**c)** Soient $E$ un $\mathbb{R}$-espace vectoriel de dimension 3 et $(e_1, e_2, e_3)$ une base de $E$. Notons $f$ l'application linéaire de $E$ dans $E$ telle que

$$\begin{cases} f(e_1) = e_1 + 2e_2 + (m+2)e_3 \\ f(e_2) = -e_1 + (m-4)e_2 - 4e_3 \\ f(e_3) = (m-2)e_1 - 2e_2 - 3e_3 \,. \end{cases}$$

Écrire la matrice de $f$ dans la base $(e_1, e_2, e_3)$.

Pour quelles valeurs de $m$ l'application $f$ est-elle bijective ? Dans ce cas, calculer la matrice de $f^{-1}$ dans la base $(e_1, e_2, e_3)$.

Pour quelles valeurs de $m$ les sous-espaces vectoriels $\operatorname{Ker} f$ et $\operatorname{Im} f$ de $E$ sont-ils supplémentaires ?

**14.** Soient $E$ un $\mathbb{R}$-espace vectoriel de dimension finie et $f$ une application linéaire de $E$ dans $E$.

**a)** Montrer que les sous-espaces vectoriels $\operatorname{Ker} f$ et $\operatorname{Im} f$ de $E$ sont supplémentaires si et seulement si $\operatorname{Ker} f \cap \operatorname{Im} f = \{0\}$.

**b)** Montrer que les sous-espaces vectoriels $\operatorname{Ker} f$ et $\operatorname{Im} f$ de $E$ sont supplémentaires si et seulement si $\operatorname{Ker} f + \operatorname{Im} f = E$.

**c)** Notons $g$ l'unique application linéaire de $\mathbb{R}^4$ dans $\mathbb{R}^4$ telle que

$$f(\mathbf{e}_1) = -2\mathbf{e}_1 - 3\mathbf{e}_4, \quad f(\mathbf{e}_2) = 10\mathbf{e}_1 + 2\mathbf{e}_2 - 6\mathbf{e}_3 + 8\mathbf{e}_4$$
$$f(\mathbf{e}_3) = 3\mathbf{e}_1 + \mathbf{e}_2 - 3\mathbf{e}_3 + \mathbf{e}_4 \quad \text{et} \quad f(\mathbf{e}_4) = 5\mathbf{e}_1 + \mathbf{e}_2 - 3\mathbf{e}_3 + 4\mathbf{e}_4,$$

où $(\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_4)$ est la base canonique de $\mathbb{R}^4$. Les sous-espaces vectoriels $\operatorname{Ker} g$ et $\operatorname{Im} g$ de $\mathbb{R}^4$ sont-ils supplémentaires ?

**15.** Soit $f$ l'application linéaire de $\mathbb{R}^3$ dans $\mathbb{R}^3$ qui à tout $(x, y, z) \in \mathbb{R}^3$ associe

$$f(x, y, z) = (-x + y + z, -6x + 4y + 2z, 3x - y + z).$$

**a)** Écrire la matrice de $f$ dans la base canonique de $\mathbb{R}^3$.

**b)** Montrer l'égalité $f \circ f = 2f$. En déduire que si $v \in \operatorname{Im} f$, alors $f(v) = 2v$.

**c)** Montrer que $\operatorname{Ker} f$ et $\operatorname{Im} f$ sont des sous-espaces vectoriels supplémentaires de $\mathbb{R}^3$.

**d)** Trouver une base $(e_1, e_2, e_3)$ de $\mathbb{R}^3$ dont le premier vecteur appartient à $\operatorname{Ker} f$ et les derniers à $\operatorname{Im} f$. Quelle est la matrice de $f$ dans la base $(e_1, e_2, e_3)$ ?

**e)** Trouver une équation de $\operatorname{Im} f$.



**16.** Soient $f : M_2(\mathbb{R}) \to \mathbb{R}$ et $g : M_2(\mathbb{R}) \to M_2(\mathbb{R})$ les applications définies par

$$f(M) = x + t \quad \text{et} \quad g(M) = \begin{bmatrix} 2x + t & x + y + t \\ x + z + t & -2x - t \end{bmatrix}$$

pour toute matrice $M = \begin{bmatrix} x & y \\ z & t \end{bmatrix}$ de $M_2(\mathbb{R})$. Posons $U = \begin{bmatrix} 1 & 1 \\ 1 & -2 \end{bmatrix}$.

**a)** Montrer que les applications $f$ et $g$ sont linéaires.

**b)** Trouver une base de $\operatorname{Ker} f$.

**c)** Calculer $g(M) - M$ lorsque $M \in \operatorname{Ker} f$. En déduire l'inclusion $\operatorname{Ker} f \subset \operatorname{Im} g$.

**d)** Calculer $g(U)$. En déduire que l'on a $\operatorname{Ker} f = \operatorname{Im} g$ et que $U$ est une base de $\operatorname{Ker} g$.

**e)** Montrer que les sous-espaces vectoriels $\operatorname{Ker} g$ et $\operatorname{Ker} f$ de $M_2(\mathbb{R})$ sont supplémentaires.

**f)** Soit $(V, W, T)$ une base de $\operatorname{Ker} f$. Écrire la matrice de $g$ dans la base $(U, V, W, T)$.

**17.** Soit $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ une matrice de $M_2(\mathbb{R})$ et soit $f : M_2(\mathbb{R}) \to M_2(\mathbb{R})$ l'application définie par $f(M) = AM - MA$ pour toute matrice $M \in M_2(\mathbb{R})$. Posons

$$E_{11} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad E_{12} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad E_{21} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \quad \text{et} \quad E_{22} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

**a)** Montrer que $f$ est une application linéaire.

**b)** Écrire la matrice de $f$ dans la base $(E_{11}, E_{12}, E_{21}, E_{22})$ de $M_2(\mathbb{R})$.

**c)** On suppose $a = d$, $c = -b$ et $b \neq 0$. Les sous-espaces vectoriels $\operatorname{Ker} f$ et $\operatorname{Im} f$ de $M_2(\mathbb{R})$ sont-ils supplémentaires ?

**d)** On suppose $a = d$, $b = 1$ et $c = 0$. Écrire la matrice de $f$ dans la base $(E_{12}, E_{22}, E_{11} + E_{22}, E_{21})$ de $M_2(\mathbb{R})$. Les sous-espaces vectoriels $\operatorname{Ker} f$ et $\operatorname{Im} f$ de $M_2(\mathbb{R})$ sont-ils supplémentaires ?

**18.** Soient $n$ un entier supérieur ou égal à 2, $E$ un $\mathbb{K}$-espace vectoriel de dimension $n$ et $(e_1, \ldots, e_n)$ une base de $E$. Soit $f$ une application linéaire de $E$ dans $E$ telle que $f(x)$ est colinéaire à $x$ pour tout $x \in E$.

**a)** Montrer que pour tout $i \in \{1, \ldots, n\}$, il existe un unique scalaire $\lambda_i$ tel que $f(e_i) = \lambda_i e_i$.

**b)** Soient $i, j \in \{1, \ldots, n\}$ tels que $i \neq j$. Calculer les coordonnées du vecteur $f(e_i + e_j)$ dans la base $(e_1, \ldots, e_n)$. En déduire $\lambda_i = \lambda_j$.

**c)** Montrer que $f$ est une homothétie.

**19.** Soit $f : \mathbf{R}^2 \to \mathbf{R}^3$ une application linéaire injective.

**a)** Montrer qu'il existe des vecteurs $u$ et $v$ appartenant à $\mathbf{R}^3$, linéairement indépendants et tels que $f(x,y) = xu + yv$ quels que soient les nombres réels $x$ et $y$.

**b)** Montrer qu'il existe un isomorphisme $g : \mathbf{R}^3 \to \mathbf{R}^3$ tel que $(g \circ f)(x,y) = (x,y,0)$ quels que soient les nombres réels $x$ et $y$.

**20.** Soient $a$ et $b$ nombres réels et soit $f : \mathbf{R}^3 \to \mathbf{R}$ la forme linéaire définie par $f(x,y,z) = ax + by + z$. Déterminer un isomorphisme $g : \mathbf{R}^3 \to \mathbf{R}^3$ tel que $(f \circ g)(x,y,z) = z$ quels que soient les nombres réels $x$, $y$ et $z$.

**21.** Soient $E$, $F$ et $G$ des $\mathbf{K}$-espaces vectoriels. Soient $f$ une application linéaire de $E$ dans $F$ et $g$ une application linéaire de $F$ dans $G$. Montrer que l'on a $g \circ f = 0$ si et seulement si $\operatorname{Im} f \subset \operatorname{Ker} g$.

**22.** Soit $E$ un $\mathbf{R}$-espace vectoriel de dimension 3. Soit $f$ une application linéaire non nulle de $E$ dans $E$, telle que $f \circ f = 0$. On note $r$ la dimension de $\operatorname{Im} f$.

**a)** Montrer l'inclusion $\operatorname{Im} f \subset \operatorname{Ker} f$. En déduire l'inégalité $r \leqslant 3 - r$. Calculer $r$.

**b)** Soit $e_1 \in E$ tel que $f(e_1) \neq 0$. On pose $e_2 = f(e_1)$. Montrer qu'il existe $e_3 \in \operatorname{Ker} f$ non colinéaire à $e_2$. Montrer que $(e_1, e_2, e_3)$ est une base de $E$. Écrire la matrice de $f$ dans cette base.

**c)** Trouver une application linéaire non nulle $g$ de $\mathbf{R}^3$ dans $\mathbf{R}^3$ telle que $g \circ g = 0$.

**23.** Soient $E$ un $\mathbf{K}$-espace vectoriel et $f$ une application linéaire de $E$ dans $E$. Pour tout entier $p \geqslant 2$, on note $f^p$ l'application linéaire de $E$ dans $E$ obtenu en composant $p$ fois $f$ avec lui-même : par exemple, on a $f^2 = f \circ f$ et $f^3 = f \circ f \circ f$. On suppose que $f^4 = 0$.

**a)** Soient $x \in E$ et $y = a_0 x + a_1 f(x) + a_2 f^2(x) + a_3 f^3(x)$, où $a_0$, $a_1$, $a_2$ et $a_3$ sont des scalaires. Calculer les vecteurs $f(y)$, $f^2(y)$ et $f^3(y)$.

**b)** Supposons qu'il existe un vecteur $x \in E$ tel que $f^3(x) \neq 0$. Montrer que les vecteurs $x, f(x), f^2(x), f^3(x)$ sont linéairement indépendants.

**c)** Supposons que l'espace vectoriel $E$ est de dimension 3. Montrer que $f^3 = 0$.

**24.** Soit $E$ un $\mathbf{R}$-espace vectoriel de dimension 2. Soit $f$ une application linéaire de $E$ dans $E$ telle que $f \circ f \circ f = \mathrm{id}_E$. On suppose qu'il existe un vecteur non nul $u \in E$ tel que $f(u)$ est colinéaire à $u$.

**a)** Montrer que l'on a $f(u) = u$.

**b)** Soit $v$ un vecteur de $E$ non colinéaire à $u$. Posons $f(v) = au + bv$ et notons $A$ la matrice de $f$ dans la base $(u,v)$. Écrire la matrice $A$ et calculer $A^3$. En déduire $f(v) = v$.

**c)** Montrer que $f = \mathrm{id}_E$.



**25.** Soit $E$ un $\mathbf{R}$-espace vectoriel de dimension 2. Soit $f$ une application linéaire de $E$ dans $E$ telle que $f \circ f \circ f = \mathrm{id}_E$. On suppose que pour tout vecteur non nul $u \in E$, $f(u)$ n'est pas colinéaire à $u$.

**a)** Montrer que $f - \mathrm{id}_E$ est un isomorphisme.

**b)** Calculer $(f - \mathrm{id}_E) \circ (\mathrm{id}_E + f + f \circ f)$. En déduire l'égalité $f \circ f = -f - \mathrm{id}_E$.

**c)** Soit $u$ un vecteur non nul de $E$. Écrire la matrice de $f$ dans la base $(u, f(u))$.

**d)** Trouver une application linéaire $g$ de $\mathbf{R}^2$ dans $\mathbf{R}^2$ qui n'est pas une homothétie et telle que $g \circ g \circ g = \mathrm{id}_{\mathbf{R}^2}$.

## Quelques réponses ou indications

1. **b)** On a $w = 3u - v$. La condition est $a = 4$.

2. Choisir un vecteur $u \in \mathbf{R}^2$ tel que $(1,1)$ et $u$ forment une base de $\mathbf{R}^2$. L'application linéaire $f : \mathbf{R}^2 \to \mathbf{R}^2$ telle que $f(1,1) = (1,2)$ et $f(u) = (a,b)$ est un isomorphisme si et seulement si $\begin{vmatrix} 1 & a \\ 2 & b \end{vmatrix} \neq 0$.

4. **b)** Le vecteur $f(w)$ doit être combinaison linéaire de $f(u)$ et $f(v)$, ce qui impose $a = -2$. Si $a = -2$, compléter $u$ et $v$ en une base de $\mathbf{R}^3$ et démontrer qu'il existe une application linéaire $f$ ayant les propriétés demandées.

6. **a)** La matrice est $\begin{bmatrix} 2 & -1 & 2 \\ 1 & 2 & 0 \\ 3 & 0 & 1 \end{bmatrix}$.

**b)** La matrice est $\begin{bmatrix} 4 & 3 & -3 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$.

8. **a)** La matrice de $s$ dans la base canonique est $\begin{bmatrix} 2 & 1 \\ -3 & -2 \end{bmatrix}$.

**d)** Une équation de $s(D)$ est $7x + 4y = 0$.

9. **b)** La matrice de $p$ est $A = \dfrac{1}{2}\begin{bmatrix} 3 & 2 & -1 \\ -1 & 0 & 1 \\ 1 & 2 & 1 \end{bmatrix}$. La matrice de $s$ est $2A - I_3$.

10. **b)** Utiliser (a) pour trouver une infinité de matrices $B \in M_2(\mathbf{R})$ telles que $B^2 = -I_2$.

11. **a)** Montrer que le vecteur $f(x)$ n'est pas colinéaire à $x$, en raisonnant par l'absurde.

12. **b)** Pour la deuxième partie de la question, montrer que $f(y)$ n'est pas combinaison linéaire de $x$, $f(x)$ et $y$, en raisonnant par l'absurde.

**d)** Calculer le carré de la matrice obtenue à la question précédente.

13. b) Ne pas oublier de traiter les cas $m=1$ et $m=2$. Lorsque $m \neq 1,2$, le système a l'unique solution :

$$\begin{cases} x = \dfrac{(3m-4)a + (4m-5)b + (m^2-6m+6)c}{(m-1)^2(m-2)} \\ y = \dfrac{2a + (m+1)b - 2c}{(m-1)(m-2)} \\ z = \dfrac{ma + b - c}{(m-1)^2}. \end{cases}$$

c) La matrice de $f$ dans la base $(e_1, e_2, e_3)$ est la matrice définie en (a). Les sous-espaces vectoriels $\operatorname{Ker} f$ et $\operatorname{Im} f$ sont supplémentaires si et seulement si $m \neq 1$.

15. e) Une équation de $\operatorname{Im} f$ est $z + y - 3x = 0$.

17. b) La matrice est $\begin{bmatrix} 0 & -c & b & 0 \\ -b & a-d & 0 & b \\ c & 0 & d-a & -c \\ 0 & c & -b & 0 \end{bmatrix}$.

19. a) On a nécessairement $u = f(1,0)$ et $v = f(0,1)$. Supposons que des nombres réels $x$ et $y$ vérifient l'égalité $xu + yv = 0$, c'est-à-dire $f(x,y) = 0$. Puisque $f$ est injective, on en déduit $(x,y) = (0,0)$.

b) Puisque les vecteurs $u$ et $v$ sont linéairement indépendants, il existe un vecteur $w \in \mathbb{R}^3$ tel que $(u, v, w)$ est une base de $\mathbb{R}^3$, d'après le théorème de la base incomplète. Définir l'application linéaire $g$ en donnant les vecteurs $g(u)$, $g(v)$ et $g(w)$. Ne pas oublier que $g$ doit être un isomorphisme.

20. L'application linéaire $g : \mathbb{R}^3 \to \mathbb{R}^3$ définie par $g(x, y, z) = (x, y, z - ax - by)$ convient, mais il y a beaucoup d'autres solutions.

22. b) On a $e_2 \in \operatorname{Ker} f$ et $\dim \operatorname{Ker} f = 2$.

23. a) Il s'agit d'exprimer chacun des vecteurs $f(y)$, $f^2(y)$ et $f^3(y)$ au moyen de $f(x)$, $f^2(x)$, $f^3(x)$.

b) Supposons que l'on a $a_0 x + a_1 f(x) + a_2 f^2(x) + a_3 f^3(x) = 0$, où les $a_i$ sont des scalaires. En appliquant $f^3$ à chaque membre de cette égalité, on obtient $a_0 f^3(x) = 0$, donc $a_0 = 0$ puisque $f^3(x)$ n'est pas le vecteur nul. Appliquer ensuite $f^2$, puis $f$.

c) Appliquer le résultat démontré à la question précédente.

25. a) Montrer que l'application $f - \mathrm{id}_E$ est injective.

b) On a $(f - \mathrm{id}_E) \circ (\mathrm{id}_E + f + f \circ f) = f \circ f \circ f - \mathrm{id}_E$.



# Chapitre 8

# Géométrie affine

Au chapitre 6, nous avons introduit le **R**-espace vectoriel $\mathbb{R}^n$ dont les éléments sont les $n$-uples $(x_1, \ldots, x_n)$ de nombres réels. Nous allons voir que les calculs et les résultats de l'algèbre linéaire dans $\mathbb{R}^2$ et $\mathbb{R}^3$ rendent compte des « propriétés affines » de la géométrie du plan et de l'espace ordinaire. Les définitions et les résultats des chapitres 4 à 7 vont être ici largement utilisés. Dans ce chapitre, $n$ est un entier positif.

## 1. Points et vecteurs

Lorsque nous appelons « point » un élément de $\mathbb{R}^n$, cela signifie que cet élément peut se représenter comme un point de la géométrie, sur une figure plane dans le cas d'un point de $\mathbb{R}^2$, à l'aide d'une « figure dans l'espace » dans le cas d'un point de $\mathbb{R}^3$. Nous emploierons des lettres capitales, comme $A$, $B$ ou $M$ pour désigner des points de $\mathbb{R}^n$. Lorsque nous ne voudrons pas interpréter un élément $v \in \mathbb{R}^n$ comme un point, nous dirons que $v$ est un vecteur, comme d'habitude pour les éléments d'un espace vectoriel.

Introduisons une notation commode.

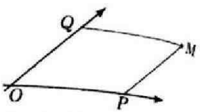
**Notation.** Soient $P$ et $Q$ des points de $\mathbb{R}^n$. On note $\overrightarrow{PQ}$ le vecteur $Q - P$.

Pour tous points $P, Q, R$ de $\mathbb{R}^n$, nous avons les propriétés :

$$(\overrightarrow{PQ} = 0 \iff P = Q), \quad \overrightarrow{PQ} = -\overrightarrow{QP} \quad \text{et} \quad \overrightarrow{PQ} + \overrightarrow{QR} = \overrightarrow{PR}.$$

Rappelons comment on peut représenter un point de $\mathbb{R}^2$ sur une figure. Dessinons un point $O$ et deux droites distinctes passant par $O$. Sur l'une des droites, faisons figurer un point $U$ différent de $O$ et sur l'autre, un point $V$ différent de $O$. On définit ainsi deux axes d'origine $O$, l'un dirigé de $O$ vers $U$, l'autre de $O$ vers $V$ et des unités de mesure $OU$ et $OV$ : ces axes s'appellent l'axe des abscisses et l'axe des ordonnées.

Soit $(x, y) \in \mathbb{R}^2$. Sur l'axe des abscisses, soit $P$ le point dont la mesure algébrique $\overline{OP}$ est égale au nombre $x$. De même, soit $Q$ le point de l'axe des ordonnées tel que $\overline{OQ} = y$. Le point $(x, y)$ est alors représenté par le point $M$ tel que le quadrilatère $OPMQ$ est un parallélogramme.




Le point $O$ représente $(0, 0)$, $P$ représente $(x, 0)$ et $Q$ représente $(0, y)$. En prenant les mêmes notations pour les points de $\mathbb{R}^2$ et les points de la figure, l'égalité $(x, y) = (x, 0) + (0, y)$ s'écrit encore $\overrightarrow{OM} = \overrightarrow{OP} + \overrightarrow{OQ}$.

## 2. Sous-espaces affines

**Définitions**

Soit $A$ un point de $\mathbb{R}^n$ et soit $V$ un sous-espace vectoriel de $\mathbb{R}^n$. L'ensemble des points $A + v$ où $v \in V$, s'appelle un *sous-espace affine de* $\mathbb{R}^n$ et plus précisément le *sous-espace affine passant par $A$ et de direction $V$*.

Si $\dim V = k$, on dit que ce sous-espace affine est de dimension $k$.

Un sous-espace affine de dimension 1 s'appelle une *droite affine* ou plus simplement une *droite*. Des points appartenant à une même droite sont dits *alignés*.

Un sous-espace affine de dimension 2 s'appelle un *plan affine* ou un *plan*.

Puisque $A = A + 0$, le point $A$ appartient heureusement à tout sous-espace affine passant par $A$.

**Proposition.** *Soit $\mathscr{V}$ un sous-espace affine de $\mathbb{R}^n$ de direction $V$ et soit $P \in \mathscr{V}$. Alors $\mathscr{V}$ est le sous-espace affine passant par $P$ et de direction $V$.*

**Démonstration.** Par hypothèse, il existe un point $A \in \mathscr{V}$ tel que $\mathscr{V}$ est l'ensemble des points $A + u$ où $u \in V$. En particulier, il existe $u_0 \in V$ tel que $P = A + u_0$, c'est-à-dire $A = P - u_0$.

Si $M$ est un point de $\mathscr{V}$, alors on a $M = A + u$ et $u \in V$, donc $M = P + (-u_0 + u)$. Puisque $u$ et $u_0$ appartiennent à $V$, on a $(-u_0 + u) \in V$, donc $M$ appartient au sous-espace affine de direction $V$ passant par $P$.

Réciproquement, pour tout $v \in V$, le point $M = P + v$ est égal à $A + (u_0 + v)$, donc $M \in \mathscr{V}$. ∎

**Corollaire.** *Si $\mathscr{V}$ est un sous-espace affine de $\mathbb{R}^n$, la direction de $\mathscr{V}$ est l'ensemble des vecteurs $\overrightarrow{PQ}$, où $P$ et $Q$ sont des points de $\mathscr{V}$.*





**Démonstration.** Supposons que $P$ est un point de $\mathscr{V}$. Si $Q \in \mathscr{V}$, alors d'après la proposition, il existe un vecteur $u \in V$ tel que $Q = P + u$ ; on a donc $u = \overrightarrow{PQ}$ et par suite $\overrightarrow{PQ} \in V$. Réciproquement, si $v \in V$, alors le point $Q = P + v$ appartient à $\mathscr{V}$ et l'on a $v = \overrightarrow{PQ}$. ∎

> Si $\mathscr{V}$ est le sous-espace affine passant par $A$ et de direction $V$, alors pour tout point $M \in \mathbb{R}^n$, on a l'équivalence
> $$M \in \mathscr{V} \iff \overrightarrow{AM} \in V.$$

**Exemples**

1) Le sous-espace affine passant par le point $A \in \mathbb{R}^n$ et de direction le sous-espace vectoriel $\{0\}$ est l'ensemble $\{A\}$.

2) Soient $A$ un point de $\mathbb{R}^n$ et $e$ un vecteur non nul de $\mathbb{R}^n$. Le sous-espace vectoriel de $\mathbb{R}^n$ engendré par $e$ est donc une droite vectorielle $D$, c'est-à-dire que l'on a $\dim D = 1$. Le sous-espace affine passant par $A$ et de direction $D$ est une droite affine. On dit que $e$ est un *vecteur directeur* de cette droite.

3) Soient $A$ et $B$ des points de $\mathbb{R}^n$ tels que $A \neq B$. Le vecteur $\overrightarrow{AB}$ est donc non nul. La droite affine passant par $A$ et de vecteur directeur $\overrightarrow{AB}$ se note $(AB)$. La droite $(AB)$ est donc l'ensemble des points $A + x\overrightarrow{AB}$, où $x \in \mathbb{R}$.

4) Supposons que $n$ est au moins égal à 2 et que $A, B, C$ sont des points non alignés de $\mathbb{R}^n$. Ces points sont nécessairement deux à deux différents, $\overrightarrow{AB}$ n'est pas le vecteur nul et $\overrightarrow{AC}$ n'est pas colinéaire à $\overrightarrow{AB}$. Les vecteurs $\overrightarrow{AB}$ et $\overrightarrow{AC}$ sont donc linéairement indépendants. Le sous-espace vectoriel $V$ engendré par $\overrightarrow{AB}$ et $\overrightarrow{AC}$ est de dimension 2, donc le sous-espace affine de $\mathbb{R}^n$ passant par $A$ et de direction $V$ est un plan, noté $(ABC)$. Un vecteur $v \in \mathbb{R}^n$ appartient à $V$ si et seulement s'il est combinaison linéaire de $\overrightarrow{AB}$ et $\overrightarrow{AC}$. Par suite, le plan $(ABC)$ est l'ensemble des points $A + x\overrightarrow{AB} + y\overrightarrow{AC}$, où $x$ et $y$ appartiennent à $\mathbb{R}$.

5) Soient $A$ un point de $\mathbb{R}^n$ et $V, W$ des sous-espaces vectoriels de $\mathbb{R}^n$. Soit $\mathscr{V}$ le sous-espace affine passant $A$ et de direction $V$ et soit $\mathscr{W}$ le sous-espace affine passant par $A$ et de direction $W$.
   - Si $V \subset W$, alors on a l'inclusion $\mathscr{V} \subset \mathscr{W}$.
   - L'intersection $\mathscr{V} \cap \mathscr{W}$ est le sous-espace affine passant par $A$ et de direction le sous-espace vectoriel $V \cap W$.

Commençons à pratiquer le langage de la géométrie en définissant la notion de sous-espaces affines parallèles.

**Définition**
On dit que des sous-espaces affines $\mathcal{V}$ et $\mathcal{W}$ de $\mathbb{R}^n$ sont *parallèles* s'ils ont la même direction. Cette relation se note $\mathcal{V} \parallel \mathcal{W}$.

Si $\mathcal{V}$ est un sous-espace affine de $\mathbb{R}^n$ et $A$ un point de $\mathbb{R}^n$, il existe un unique sous-espace affine passant par $A$ et parallèle à $\mathcal{V}$ : le sous-espace affine passant par $A$ dont la direction est celle de $\mathcal{V}$.

**Proposition.** *Soient $\mathcal{V}$ et $\mathcal{W}$ des sous-espaces affines de $\mathbb{R}^n$. Si $\mathcal{V}$ et $\mathcal{W}$ sont parallèles, alors ou bien $\mathcal{V} = \mathcal{W}$, ou bien $\mathcal{V} \cap \mathcal{W}$ est l'ensemble vide.*

**Démonstration.** Supposons les sous-espaces affines $\mathcal{V}$ et $\mathcal{W}$ parallèles, donc de même direction $V$. Supposons qu'il existe un point $A \in \mathcal{V} \cap \mathcal{W}$. D'après la proposition précédente, $\mathcal{V}$ est le sous-espace affine passant par $A$ et de direction $V$ ; de même, $\mathcal{W}$ est le sous-espace affine passant par $A$ et de direction $V$. On a donc $\mathcal{V} = \mathcal{W}$. ∎

**Corollaire.** *Soient $A$ et $B$ des points de $\mathbb{R}^n$ tels que $A \neq B$. Si $C$ et $D$ sont des points différents appartenant à la droite $(AB)$, alors $(CD) = (AB)$.*

*Supposons $n \geqslant 2$. Soient $A, B, C$ des points non alignés de $\mathbb{R}^n$. Si $P, Q, R$ sont des points non alignés appartenant au plan $(ABC)$, alors $(PQR) = (ABC)$.*

**Démonstration.** Puisque les points $C$ et $D$ appartiennent à la droite $(AB)$, le vecteur $\overrightarrow{CD}$ appartient à la direction de $(AB)$ donc est colinéaire à $\overrightarrow{AB}$. Puisque $C \neq D$, $\overrightarrow{CD}$ est un vecteur directeur de la droite $(AB)$. Les droites $(CD)$ et $(AB)$ sont donc parallèles. Puisque le point $C$ appartient à $(CD)$ et à $(AB)$, on a $(CD) = (AB)$ d'après la proposition précédente.

Le raisonnement est semblable dans le cas d'un plan. Puisque $P, Q, R$ appartiennent au plan $(ABC)$ et sont des points non alignés, la direction du plan $(ABC)$ est le plan vectoriel engendré par $\overrightarrow{PQ}$ et $\overrightarrow{PR}$. Les plans $(PQR)$ et $(ABC)$ sont donc parallèles. Il s'ensuit $(PQR) = (ABC)$, car $P \in (ABC)$. ∎

Voici des résultats généraux concernant l'intersection de deux sous-espaces affines.

**Proposition.** *Soient $A$ un point de $\mathbb{R}^n$ et $V, W$ des sous-espaces vectoriels de $\mathbb{R}^n$. Soit $\mathcal{V}$ le sous-espace affine de $\mathbb{R}^n$ passant par $A$ et de direction $V$ et soit $\mathcal{W}$ le sous-espace affine de $\mathbb{R}^n$ passant par $A$ et de direction $W$. Si $V \cap W = \{0\}$, alors $\mathcal{V} \cap \mathcal{W} = \{A\}$.*

**Démonstration.** Le sous-espace affine $\mathcal{V} \cap \mathcal{W}$ passe par $A$ et sa direction est le sous-espace vectoriel $V \cap W = \{0\}$. ∎





**Proposition.** *Soient $A, B$ des points de $\mathbb{R}^n$ et $V, W$ des sous-espaces vectoriels de $\mathbb{R}^n$. Soit $\mathcal{V}$ le sous-espace affine de $\mathbb{R}^n$ passant par $A$ et de direction $V$ et soit $\mathcal{W}$ le sous-espace affine de $\mathbb{R}^n$ passant par $B$ et de direction $W$. On a l'équivalence*

$$\overrightarrow{AB} \in V + W \iff \mathcal{V} \cap \mathcal{W} \neq \varnothing.$$

**Démonstration.** Supposons qu'il existe un point $M \in \mathcal{V} \cap \mathcal{W}$. Puisque $A$ appartient à $\mathcal{V}$, le vecteur $\overrightarrow{AM}$ appartient à $V$. De même, le vecteur $\overrightarrow{MB}$ appartient à $W$. Le vecteur $\overrightarrow{AB} = \overrightarrow{AM} + \overrightarrow{MB}$ appartient donc au sous-espace vectoriel $V + W$. Réciproquement, supposons que l'on a $\overrightarrow{AB} \in V + W$, c'est-à-dire qu'il existe des vecteurs $v \in V$ et $w \in W$ tels que $\overrightarrow{AB} = v + w$. Il vient $B - A = v + w$ ou encore $A + v = B - w$. Le point $A + v$ appartient à $\mathcal{V}$ et le point $B - w$ appartient à $\mathcal{W}$, par suite le point $A + v$ appartient à $\mathcal{V} \cap \mathcal{W}$. ∎

**Corollaire.** *Soient $\mathcal{V}$ et $\mathcal{W}$ des sous-espaces affines de $\mathbb{R}^n$, de direction respective $V$ et $W$. Si les sous-espaces vectoriels $V$ et $W$ sont supplémentaires, alors il existe un point $P \in \mathbb{R}^n$ tel que $\mathcal{V} \cap \mathcal{W} = \{P\}$.*

**Démonstration.** Choisissons un point $A \in \mathcal{V}$ et un point $B \in \mathcal{W}$. Puisque $V + W = \mathbb{R}^n$, le vecteur $\overrightarrow{AB}$ appartient à $V + W$. D'après la proposition précédente, il existe un point $P \in \mathcal{V} \cap \mathcal{W}$. Les sous-espaces affines $\mathcal{V}$ et $\mathcal{W}$ passent par $P$ et l'on a $V \cap W = \{0\}$, par suite $\mathcal{V} \cap \mathcal{W} = \{P\}$, d'après une proposition ci-dessus. ∎

**Exemples**

1) Choisissons une base $(e_1, e_2, e_3, e_4)$ de $\mathbb{R}^4$ et des points $A, B$ de $\mathbb{R}^4$. Notons $V$ le sous-espace vectoriel engendré par $e_1, e_2$ et $W$ le sous-espace vectoriel engendré par $e_3, e_4$ ; ces sous-espaces vectoriels sont de dimension 2. Le plan $\mathcal{V}$ passant par $A$ et de direction $V$ est l'ensemble des points $A + xe_1 + ye_2$, où $x, y \in \mathbb{R}$ et le plan $\mathcal{W}$ passant par $B$ et de direction $W$ est l'ensemble des points $B + ze_3 + te_4$, où $z, t \in \mathbb{R}$. Puisque $(e_1, e_2, e_3, e_4)$ est une base de $\mathbb{R}^4$, les sous-espaces vectoriels $V$ et $W$ sont supplémentaires. Les deux plans $\mathcal{V}$ et $\mathcal{W}$ ont donc exactement un point en commun.

2) Soient $V$ un sous-espace vectoriel de dimension 2 de $\mathbb{R}^3$, $A$ un point de $\mathbb{R}^3$ et $\mathcal{V}$ le sous-espace affine passant par $A$ et de direction $V$. Puisque $\dim V = 2$, $\mathcal{V}$ est un plan. Soit $B$ un point de $\mathbb{R}^3$ tel que $B \notin \mathcal{V}$ et soit $u$ un vecteur non nul de $V$. Notons $D$ la droite vectorielle engendrée par $u$ et $\mathcal{D}$ la droite affine passant par $B$ et de direction $D$. Puisque $u \in V$, on a $D \subset V$ donc $D + V = V$. Puisque $A \in \mathcal{V}$ et $B \notin \mathcal{V}$, le vecteur $\overrightarrow{AB}$ n'appartient pas à $V$. D'après la proposition précédente, il s'ensuit $\mathcal{D} \cap \mathcal{V} = \varnothing$.

**Exercice.** Considérons les points de $\mathbb{R}^3$ : $A=(0,1,-1)$, $B=(2,-5,8)$ et $C=(1,1,-1)$.

a) Notons $\mathscr{V}$ l'ensemble des points $(2+x+y,-1-2x,2+3x)$, où $x,y \in \mathbb{R}$. Montrer que $\mathscr{V}$ est un plan affine de $\mathbb{R}^3$.

b) Montrer que les points $A, B, C$ sont non alignés et que $\mathscr{V}$ est le plan $(ABC)$.

c) Notons $\mathscr{D}$ l'ensemble des points $(2x-2, 5-2x, -7+3x)$, où $x \in \mathbb{R}$. Montrer que $\mathscr{D}$ est une droite affine contenue dans le plan $(ABC)$.

**Réponse**

a) Posons $O=(2,-1,2)$, $e_1=(1,-2,3)$ et $e_2=(1,0,0)$, de sorte que pour tous nombres réels $x, y$, nous avons

$$(2+x+y,-1-2x,2+3x)=(2,-1,2)+x(1,-2,3)+y(1,0,0)=O+xe_1+ye_2.$$

Notons $V$ le sous-espace vectoriel de $\mathbb{R}^3$ engendré par $e_1$ et $e_2$. L'ensemble $\mathscr{V}$ est le sous-espace affine passant par $O$ et de direction $V$. Les vecteurs $e_1$ et $e_2$ sont linéairement indépendants, par suite $\dim V = 2$ et $\mathscr{V}$ est un plan.

b) Nous avons $\overrightarrow{AB} = B - A = (2,-6,9)$ et $\overrightarrow{AC} = C - A = (1,0,0)$, donc les vecteurs $\overrightarrow{AB}$ et $\overrightarrow{AC}$ sont linéairement indépendants. Il s'ensuit que les points $A, B, C$ sont non alignés. Montrons que les points $A, B, C$ appartiennent à $\mathscr{V}$. Puisque $O$ est un point de $\mathscr{V}$, cela revient à démontrer que les vecteurs $\overrightarrow{OA}$, $\overrightarrow{OB}$ et $\overrightarrow{OC}$ appartiennent à $V$. Or nous avons $\overrightarrow{OA} = A - O = (-2,2,-3)$. Calculons le déterminant de la matrice de $M_3(\mathbb{R})$ dont les colonnes sont les coordonnées des vecteurs $e_1$, $e_2$ et $\overrightarrow{OA}$ dans la base canonique de $\mathbb{R}^3$. Il vient

$$\begin{vmatrix} 1 & 1 & -2 \\ -2 & 0 & 2 \\ 3 & 0 & -3 \end{vmatrix} = -\begin{vmatrix} -2 & 2 \\ 3 & -3 \end{vmatrix} = 0.$$

Les vecteurs $e_1$, $e_2$ et $\overrightarrow{OA}$ ne forment donc pas une base de $\mathbb{R}^3$, par suite ne sont pas linéairement indépendants. Puisque $e_1$ et $e_2$ le sont, on en déduit que $\overrightarrow{OA}$ est combinaison linéaire de $e_1$ et $e_2$, donc appartient à $V$. De même, nous avons $\overrightarrow{OB} = B - O = (0,-4,6)$, $\overrightarrow{OC} = (-1,2,-3)$,

$$\begin{vmatrix} 1 & 1 & 0 \\ -2 & 0 & -4 \\ 3 & 0 & 6 \end{vmatrix} = -\begin{vmatrix} -2 & -4 \\ 3 & 6 \end{vmatrix} = 0 \quad \text{et} \quad \begin{vmatrix} 1 & 1 & -1 \\ -2 & 0 & 2 \\ 3 & 0 & -3 \end{vmatrix} = -\begin{vmatrix} -2 & 2 \\ 3 & -3 \end{vmatrix} = 0.$$

Les vecteurs $\overrightarrow{OB}$ et $\overrightarrow{OC}$ sont donc combinaison linéaire de $e_1$ et $e_2$. Les points $A, B, C$ appartiennent ainsi au plan $\mathscr{V}$. Il s'ensuit que $\mathscr{V}$ est le plan $(ABC)$.

c) Posons $P = (-2,5,-7)$ et $u = (2,-2,3)$. Pour tout nombre réel $x$, nous avons

$$(2x-2, 5-2x, -7+3x) = (-2,5,-7) + x(2,-2,3) = P + xu.$$

Puisque $u$ n'est pas le vecteur nul, $\mathscr{D}$ est la droite affine passant par $P$ et de vecteur directeur $u$. Montrons que le vecteur $\overrightarrow{AP}$ est combinaison linéaire des vecteurs $\overrightarrow{AB}$ et $\overrightarrow{AC}$. Nous avons $\overrightarrow{AP} = P - A = (-2,4,-6)$ et le déterminant de la matrice dont les colonnes sont les coordonnées des vecteurs $\overrightarrow{AB}$, $\overrightarrow{AC}$ et $\overrightarrow{AP}$



dans la base canonique de $\mathbb{R}^3$ est donc

$$\begin{vmatrix} 2 & 1 & -2 \\ -6 & 0 & 4 \\ 9 & 0 & -6 \end{vmatrix} = -\begin{vmatrix} -6 & 4 \\ 9 & -6 \end{vmatrix} = 0.$$

Puisque les vecteurs $\overrightarrow{AB}$ et $\overrightarrow{AC}$ sont linéairement indépendants, on en déduit que $\overrightarrow{AP}$ est combinaison linéaire de $\overrightarrow{AB}$ et $\overrightarrow{AC}$. Il s'ensuit que le point $P$ appartient au plan $(ABC)$. D'autre part, nous avons $u = \overrightarrow{AO}$. Les points $A$ et $O$ appartenant au plan $(ABC)$, on en déduit $u \in V$. La droite $\mathscr{D}$ est donc contenue dans le plan $(ABC)$.

## 3. Repères et barycentre

**Définition**

Soit $\mathscr{V}$ un sous-espace affine de $\mathbb{R}^n$ de direction $V$. Si $\dim V = k$, où $k$ est un entier positif, un *repère cartésien* de $\mathscr{V}$ est un $(k+1)$-uple noté $(O; e_1, \dots, e_k)$ formé d'un point $O \in \mathscr{V}$ et d'une base $(e_1, \dots, e_k)$ de l'espace vectoriel $V$.

Supposons que $(O; e_1, \dots, e_k)$ est un repère cartésien du sous-espace affine $\mathscr{V}$. Pour tout point $M \in \mathscr{V}$, nous avons $\overrightarrow{OM} \in V$ donc il existe des nombres réels $x_1, \dots, x_k$ uniques tels que $\overrightarrow{OM} = x_1e_1 + \cdots + x_ke_k$. Ces nombres s'appellent les *coordonnées* du point $M$ dans le repère $(O; e_1, \dots, e_k)$.

**Exemple.** Si $A$ et $B$ sont des points différents de $\mathbb{R}^n$, alors $(A; \overrightarrow{AB})$ est un repère cartésien de la droite $(AB)$ et pour tout $x \in \mathbb{R}$, le point de coordonnée $x$ dans ce repère est le point $A + x\overrightarrow{AB}$.

**Définition**

Soit $(O; e)$ un repère cartésien d'une droite affine $\mathscr{D}$. Si $P$ et $Q$ sont des points de $\mathscr{D}$, le nombre réel $t$ tel que $\overrightarrow{PQ} = te$ se note $\overline{PQ}$ et s'appelle la *mesure algébrique* de $(P, Q)$ dans ce repère.

**Proposition.** *Soient $\mathscr{D}$ une droite affine de $\mathbb{R}^n$ et $P, Q, P', Q'$ des points de $\mathscr{D}$ tels que $P \neq Q$. Le nombre $\dfrac{\overline{P'Q'}}{\overline{PQ}}$ ne dépend pas du repère cartésien de $\mathscr{D}$ que l'on choisit.*

**Démonstration.** Soient $(O; e)$ et $(O_1; e_1)$ des repères cartésiens de $\mathscr{D}$. Soient $t, t', t_1, t'_1$ les nombres réels définis par $\overrightarrow{PQ} = te = t_1e_1$ et $\overrightarrow{P'Q'} = t'e = t'_1e_1$. Puisque $e$ et $e_1$ sont des vecteurs directeurs de $\mathscr{D}$, il existe un nombre réel $\lambda \neq 0$ tel que $e_1 = \lambda e$. On a $t = t_1\lambda$, $t' = t'_1\lambda$ et puisque $\overrightarrow{PQ}$ n'est pas le vecteur nul, $t$ et $t_1$ sont non nuls. Il vient donc $t'/t = t'_1/t_1$. ■

Soit $(O; e_1, \dots, e_k)$ un repère cartésien du sous-espace affine $\mathscr{V}$. Pour tout entier $i$ compris entre 1 et $k$, posons $A_i = O + e_i$. Soit $M \in \mathscr{V}$ le point de coordonnées $(x_1, \dots, x_k)$. L'égalité $\overrightarrow{OM} = x_1 e_1 + \cdots + x_k e_k$ s'écrit sous les formes équivalentes

$$M = O + x_1 e_1 + \cdots + x_k e_k \iff M = O + x_1(A_1 - O) + \cdots + x_k(A_k - O)$$
$$\iff M = (1 - x_1 \cdots - x_k)O + x_1 A_1 + \cdots + x_k A_k.$$

Pour tout point $M \in \mathscr{V}$, il existe donc des nombres réels $x_0, x_1, \dots, x_k$ tels que

$$M = x_0 O + x_1 A_1 + \cdots + x_k A_k \quad \text{et} \quad x_0 + x_1 + \cdots + x_k = 1.$$

Nous allons maintenant étudier la signification géométrique de telles combinaisons linéaires de points.

**Définitions**

Soient $p$ un entier positif, $A_1, \dots, A_p$ des points de $\mathbb{R}^n$ et $a_1, \dots, a_p$ des nombres réels tels que $a_1 + \cdots + a_p \neq 0$. Le point $G = \dfrac{1}{a_1 + \cdots + a_p}(a_1 A_1 + \cdots + a_p A_p)$ s'appelle le *barycentre des points* $A_1, \dots, A_p$ *affectés des coefficients* $a_1, \dots, a_p$.

Si tous les coefficients sont égaux à 1, on dit que le point $G = \dfrac{1}{p}(A_1 + \cdots + A_p)$ est l'*isobarycentre* des points $A_1, \dots, A_p$. Si $p = 2$, l'isobarycentre des points $A_1, A_2$ s'appelle le *milieu* de $A_1 A_2$.

**Remarques**

- On obtient aussi l'isobarycentre en choisissant tous les coefficients égaux à un même nombre $a$ non nul quelconque : en effet, on a

$$\frac{1}{pa}(aA_1 + \cdots + aA_p) = \frac{1}{p}(A_1 + \cdots + A_p).$$

- Posons $s = a_1 + \cdots + a_p$. L'égalité $\frac{1}{s}(a_1 A_1 + \cdots + a_p A_p) = \frac{a_1}{s} A_1 + \cdots + \frac{a_p}{s} A_p$ montre que $G$ est aussi le barycentre des points $A_1, \dots, A_p$ affectés des coefficients $\alpha_i = a_i / s$. On a alors $\alpha_1 + \cdots + \alpha_p = 1$.

**Proposition.** *Soient $A_1, \dots, A_p$ des points de $\mathbb{R}^n$ et $a_1, \dots, a_p$ des nombres réels tels que $a_1 + \cdots + a_p \neq 0$. Le barycentre des points $A_1, \dots, A_p$ affectés des coefficients $a_1, \dots, a_p$ est l'unique point $G$ tel que $a_1 \overrightarrow{GA_1} + \cdots + a_p \overrightarrow{GA_p} = 0$. De plus, pour tout point $M \in \mathbb{R}^n$, on a $(a_1 + \cdots + a_p)\overrightarrow{MG} = a_1 \overrightarrow{MA_1} + \cdots + a_p \overrightarrow{MA_p}$.*



**Démonstration.** On a $a_1 A_1 + \cdots + a_p A_p = (a_1 + \cdots + a_p)G = a_1 G + \cdots + a_p G$, donc $0 = a_1(A_1 - G) + \cdots + a_p(A_p - G) = a_1 \overrightarrow{GA_1} + \cdots + a_p \overrightarrow{GA_p}$. Pour tout point $M \in \mathbb{R}^n$, il vient

$$a_1 \overrightarrow{MA_1} + \cdots + a_p \overrightarrow{MA_p} = a_1(\overrightarrow{MG} + \overrightarrow{GA_1}) + \cdots + a_p(\overrightarrow{MG} + \overrightarrow{GA_p})$$
$$= (a_1 + \cdots + a_p)\overrightarrow{MG} + a_1 \overrightarrow{GA_1} + \cdots + a_p \overrightarrow{GA_p}$$
$$= (a_1 + \cdots + a_p)\overrightarrow{MG}$$

puisque $a_1 \overrightarrow{GA_1} + \cdots + a_p \overrightarrow{GA_p}$ est le vecteur nul.

Il reste à montrer que si $H$ est un point de $\mathbb{R}^n$ tel que $a_1 \overrightarrow{HA_1} + \cdots + a_p \overrightarrow{HA_p} = 0$, alors $H = G$. Appliquons ce que nous venons de démontrer au point $M = H$. Il vient $(a_1 + \cdots + a_p)\overrightarrow{HG} = a_1 \overrightarrow{HA_1} + \cdots + a_p \overrightarrow{HA_p} = 0$. Puisque le nombre $a_1 + \cdots + a_p$ n'est pas nul, on en déduit que $\overrightarrow{HG}$ est le vecteur nul, c'est-à-dire $H = G$. ∎

**Proposition.** *Si $\mathscr{V}$ est un sous-espace affine de $\mathbb{R}^n$, alors tout barycentre de points de $\mathscr{V}$ est un point de $\mathscr{V}$.*

**Démonstration.** Soit $\mathscr{V}$ un sous-espace affine de $\mathbb{R}^n$, de direction $V$. Soient $p$ un entier supérieur ou égal à 2, $A_1, \dots, A_p$ des points de $\mathscr{V}$ et $G$ leur barycentre affectés des coefficients $a_1, \dots, a_p$. Posons $s = a_1 + \cdots + a_p$. Pour tout point $M \in \mathbb{R}^n$, nous avons $s\overrightarrow{MG} = a_1 \overrightarrow{MA_1} + \cdots + a_p \overrightarrow{MA_p}$. En particulier pour le point $M = A_1$, il vient

$$s\overrightarrow{A_1G} = a_1 \overrightarrow{A_1A_1} + a_2 \overrightarrow{A_1A_2} + \cdots + a_p \overrightarrow{A_1A_p} = a_2 \overrightarrow{A_1A_2} + \cdots + a_p \overrightarrow{A_1A_p}$$

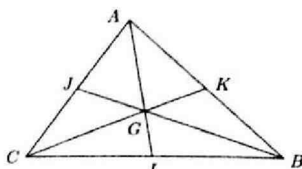
car $\overrightarrow{A_1A_1}$ est le vecteur nul. Puisque les points $A_1, \dots, A_p$ appartiennent à $\mathscr{V}$, les vecteurs $\overrightarrow{A_1A_2}, \dots, \overrightarrow{A_1A_p}$ appartiennent à $V$ et il en va de même de toute combinaison linéaire de ces vecteurs. Par conséquent le vecteur $s\overrightarrow{A_1G}$ appartient à $V$, donc aussi le vecteur $\overrightarrow{A_1G}$ puisque $s$ est différent de 0. On en déduit que le point $G$ appartient à $\mathscr{V}$. ∎

**Associativité du barycentre.** *Soient $p$ et $q$ des entiers positifs tels que $q < p$, $A_1, \dots, A_p$ des points de $\mathbb{R}^n$ et $a_1, \dots, a_p$ des nombres réels tels que les sommes $a_1 + \cdots + a_p$, $s_1 = a_1 + \cdots + a_q$ et $s_2 = a_{q+1} + \cdots + a_p$ sont toutes non nulles. Soient $G_1$ le barycentre des points $A_1, \dots, A_q$ affectés des coefficients $a_1, \dots, a_q$ et $G_2$ le barycentre des points $A_{q+1}, \dots, A_p$ affectés des coefficients $a_{q+1}, \dots, a_p$. Alors le barycentre des points $A_1, \dots, A_p$ affectés des coefficients $a_1, \dots, a_p$ est le barycentre des points $G_1$ et $G_2$ affectés des coefficients $s_1$ et $s_2$.*

**Démonstration.** Notons $G$ le barycentre des points $A_1, \dots, A_p$ affectés des coefficients $a_1, \dots, a_p$ : on a $(a_1 + \cdots + a_p)G = a_1 A_1 + \cdots + a_q A_q$. Par définition des points $G_1$ et $G_2$, on a $s_1 G_1 = a_1 A_1 + \cdots + a_q A_q$ et $s_2 G_2 = a_{q+1} A_{q+1} + \cdots + a_p A_p$. Ajoutons ces deux égalités. Il vient $s_1 G_1 + s_2 G_2 = a_1 A_1 + \cdots + a_p A_p = (a_1 + \cdots + a_p)G = (s_1 + s_2)G$. Il s'ensuit que $G$ est le barycentre de $G_1$ et $G_2$ affectés des coefficients $s_1$ et $s_2$. ∎

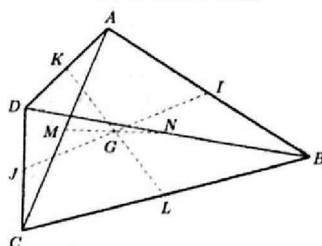
**Exemples**

1) Soient $A, B, C$ des points non alignés de $\mathbb{R}^2$. Notons $I$ le milieu de $BC$, $J$ le milieu de $CA$ et $K$ le milieu de $AB$. Alors les droites $(AI)$, $(BJ)$ et $(CK)$ ont en commun un point et un seul. Ces droites s'appellent les *médianes du triangle* $ABC$ et l'affirmation précédente est le théorème bien connu : *les médianes d'un triangle sont concourantes.*




Démontrons ce résultat. Puisque les points $A, B, C$ ne sont pas alignés, ils sont deux à deux différents et aucun d'eux n'appartient à la droite définie par les deux autres. Le point $I$ est barycentre de $B$ et $C$ donc appartient à la droite $(BC)$, donc est différent de $A$. La droite $(AI)$ est ainsi bien définie. De même, $J$ appartient à $(CA)$, $K$ appartient à $(AB)$ et les droites $(BJ)$ et $(CK)$ sont bien définies. Notons $G$ l'isobarycentre des points $A, B, C$, c'est-à-dire le barycentre de $A, B, C$ affectés de coefficients tous égaux à 1. D'après l'associativité du barycentre, $G$ est aussi le barycentre des points $A$ et $I$ affectés des coefficients 1 et 2, donc $G$ appartient à la droite $(AI)$. De même, $G$ appartient à la droite $(BJ)$ et à la droite $(CK)$. Les droites $(AI)$, $(BJ)$ et $CK)$ n'ont qu'un seul point en commun, sinon ces droites seraient égales et les points $A, B, C$ appartiendraient à cette droite, contrairement à l'hypothèse.

2) Soit $ABCD$ un quadrilatère de $\mathbb{R}^2$. Notons $I$ le milieu de $AB$, $J$ le milieu de $CD$, $K$ le milieu de $AD$, $L$ le milieu de $BC$, $M$ le milieu de $AC$ et $N$ le milieu de $BD$. Alors $IJ$, $KL$ et $MN$ ont le même milieu.






En effet, notons $G$ l'isobarycentre des points $A, B, C, D$. D'après l'associativité du barycentre, $G$ est aussi le barycentre des points $I$ et $J$ affectés du même coefficient 2, donc $G$ est le milieu de $IJ$. De même, $G$ est le milieu de $KL$ et le milieu de $MN$.

**Définition**

Soit $\mathcal{V}$ un sous-espace affine de $\mathbb{R}^n$ de dimension $k$, où $k$ est un entier positif. Un *repère affine* de $\mathcal{V}$ est un $(k+1)$-uple $(A_0, \ldots, A_k)$ de points de $\mathcal{V}$ tels que les vecteurs $\overrightarrow{A_0A_1}, \ldots, \overrightarrow{A_0A_k}$ forment une base de $V$, la direction de $\mathcal{V}$.

Si $(A_0, \ldots, A_k)$ est un repère affine de $\mathcal{V}$, alors $(A_0; \overrightarrow{A_0A_1}, \ldots, \overrightarrow{A_0A_k})$ est un repère cartésien de $\mathcal{V}$.

Si $(O; e_1, \ldots, e_k)$ est un repère cartésien de $\mathcal{V}$, alors $(O, O+e_1, \ldots, O+e_k)$ est un repère affine de $\mathcal{V}$.

**Exemples**

- Si $A$ et $B$ sont des points de $\mathbb{R}^n$ tels que $A \neq B$, alors $(A; \overrightarrow{AB})$ est un repère cartésien de la droite $(AB)$ et le couple $(A, B)$ en est un repère affine.
- Soient $A, B, C$ des points non alignés de $\mathbb{R}^n$. Alors $(A; \overrightarrow{AB}, \overrightarrow{AC})$ est un repère cartésien du plan $(ABC)$ et $(A, B, C)$ en est un repère affine. Le triplet $(B, A, C)$ est un autre repère affine du plan $(ABC)$. En effet, les vecteurs $\overrightarrow{BA} = -\overrightarrow{AB}$ et $\overrightarrow{BC} = \overrightarrow{AC} - \overrightarrow{AB}$ sont linéairement indépendants puisque $\overrightarrow{AB}$ et $\overrightarrow{AC}$ le sont.

**Proposition.** *Soient $k$ un entier positif, $\mathcal{V}$ un sous-espace affine de $\mathbb{R}^n$ de dimension $k$ et $(A_0, \ldots, A_k)$ un repère affine de $\mathcal{V}$. Pour tout point $M \in \mathcal{V}$, il existe des nombres réels $a_0, \ldots, a_k$ uniques tels que $a_0 + \cdots + a_k = 1$ et $M = a_0A_0 + \cdots + a_kA_k$.*

**Démonstration.** Nous avons déjà démontré au début du paragraphe l'existence des nombres $a_i$. Rappelons ce calcul. Soient $x_0, \ldots, x_k$ les coordonnées de $M$ dans le repère cartésien $(A_0; \overrightarrow{A_0A_1}, \ldots, \overrightarrow{A_0A_k})$. On a donc $M - A_0 = \overrightarrow{A_0M} = x_1\overrightarrow{A_0A_1} + \cdots + x_k\overrightarrow{A_0A_k}$ c'est-à-dire

$$\begin{aligned} M &= A_0 + x_1(A_1 - A_0) + \cdots + x_k(A_k - A_0) \\ &= (1 - x_1 - \cdots - x_k)A_0 + x_1A_1 + \cdots + x_kA_k. \end{aligned}$$

En posant $a_0 = 1 - x_1 - \cdots - x_k, a_1 = x_1, \ldots, a_k = x_k$, il vient $a_0 + a_1 + \cdots + a_k = 1$ et $M = a_0A_0 + \cdots + a_kA_k$.

Pour montrer que les nombres $a_0, \ldots, a_k$ sont uniques, supposons que l'on a $a_0A_0 + \cdots + a_kA_k = b_0A_0 + \cdots + b_kA_k$ et $a_0 + \cdots + a_k = b_0 + \cdots + b_k = 1$. On en déduit

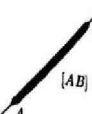
$$a_0\overrightarrow{A_0A_0} + a_1\overrightarrow{A_0A_1} + \cdots + a_k\overrightarrow{A_0A_k} = b_0\overrightarrow{A_0A_0} + b_1\overrightarrow{A_0A_1} + \cdots + b_k\overrightarrow{A_0A_k}$$

c'est-à-dire $(a_1 - b_1)\overrightarrow{A_0A_1} + \cdots + (a_k - b_k)\overrightarrow{A_0A_k} = 0$ et par suite $a_i - b_i = 0$ pour tout entier $i$ tel que $1 \leqslant i \leqslant k$. Puisque la somme des $a_i$ est égale à la somme des $b_i$, il s'ensuit $a_0 = b_0$. ∎

D'après cette proposition, tout point de $\mathcal{V}$ est barycentre de $A_0, \ldots, A_k$ et les coefficients sont bien déterminés pourvu que leur somme soit égale à 1.

**Exemple.** Si $A$ et $B$ sont des points distincts de $\mathbb{R}^n$, tout point $M$ de la droite $(AB)$ s'écrit de manière unique $M = tA + (1-t)B$ où $t \in \mathbb{R}$. Cette égalité exprime que $M$ est le barycentre des points $A$ et $B$ affectés des coefficients $t$ et $1-t$, autrement dit nous avons l'égalité vectorielle $t\overrightarrow{MA} + (1-t)\overrightarrow{MB} = 0$.

**Définition**
Soient $A$ et $B$ des points de $\mathbb{R}^n$. Le *segment* $[AB]$ est l'ensemble des points $tA + (1-t)B$ où $t$ est un nombre réel tel que $0 \leqslant t \leqslant 1$.




## 4. Géométrie affine dans le plan

Étudions plus précisément les sous-espaces affines de $\mathbb{R}^2$. Puisque les sous-espaces vectoriels de $\mathbb{R}^2$ sont de dimension 0, 1 ou 2, les sous-espaces affines de $\mathbb{R}^2$ sont :
- les parties $\{A\}$ à un élément (dimension 0),
- les droites (dimension 1),
- l'ensemble $\mathbb{R}^2$ tout entier.

On dit que des droites sont *sécantes* (au point $A$), ou qu'elles *se coupent* en $A$, si leur intersection est $\{A\}$.

**Proposition.** *Deux droites de $\mathbb{R}^2$ sont sécantes ou parallèles.*

**Démonstration.** Soient $\mathcal{D}$ et $\mathcal{D}'$ des droites de $\mathbb{R}^2$. Notons $D$ la direction de $\mathcal{D}$ et $D'$ la direction de $\mathcal{D}'$. Si $D = D'$, alors par définition les droites $\mathcal{D}$ et $\mathcal{D}'$ sont parallèles. Supposons $D \neq D'$ et choisissons un vecteur non nul $e \in D$ et un vecteur non nul $e' \in D'$. Puisque les droites vectorielles $D$ et $D'$ ne sont pas égales, le vecteur $e'$ n'est pas colinéaire à $e$, donc $(e, e')$ est une base de $\mathbb{R}^2$. Par conséquent on a $\mathbb{R}^2 = D \oplus D'$. On en déduit, d'après le corollaire page 161, qu'il existe un point $A$ tel que $\mathcal{D} \cap \mathcal{D}' = \{A\}$. ∎

Dans la suite du paragraphe, nous choisissons un repère cartésien $(O; i, j)$ de $\mathbb{R}^2$. Les points ont leur coordonnées dans ce repère et les vecteurs ont leurs coordonnées dans la base $(i, j)$ de $\mathbb{R}^2$.





### Équation d'une droite

Soit $A$ le point de $\mathbb{R}^2$ de coordonnées $a, b$, c'est-à-dire $A = O + ai + bj$, et soit $e$ le vecteur non nul de coordonnées $r, s$, c'est-à-dire $e = ri + sj$ où les nombres $r$ et $s$ ne sont pas tous deux nuls. Notons $\mathcal{D}$ la droite passant par $A$ et de vecteur directeur $e$. Pour tout point $M$ de coordonnées $x, y$, nous avons $M = O + xi + yj$ donc

$$\overrightarrow{AM} = M - A = (xi + yj) - (ai + bj) = (x-a)i + (y-b)j.$$

On en déduit les équivalences

$$M \in \mathcal{D} \iff \overrightarrow{AM} \text{ est colinéaire à } e$$
$$\iff \begin{vmatrix} x-a & r \\ y-b & s \end{vmatrix} = 0$$
$$\iff s(x-a) - r(y-b) = 0.$$

Nous venons d'écrire une équation de la droite passant par $A$ et de vecteur directeur $e$. En développant, cette équation s'écrit $sx - ry + w = 0$.

Pour trouver l'équation d'une droite passant par deux points différents $A$ et $A'$, on choisit (par exemple) le vecteur $\overrightarrow{AA'}$ comme vecteur directeur ; si les coordonnées du point $A'$ sont $a', b'$, celles du vecteur $\overrightarrow{AA'} = A' - A$ sont $a' - a, b' - b$.

> Les droites affines de $\mathbb{R}^2$ ont pour équation $ux + vy + w = 0$, où les nombres $u$ et $v$ ne sont pas tous deux nuls.
> La droite d'équation $ux + vy + w = 0$ a pour vecteur directeur $(-v, u)$.

### Droites parallèles

Soit $\mathcal{D}$ la droite d'équation $ux + vy + w = 0$ et soit $\mathcal{D}'$ la droite d'équation $u'x + v'y + w' = 0$. Les nombres $u$ et $v$ ne sont pas tous deux nuls, non plus que les nombres $u'$ et $v'$. D'après ce que nous venons de voir, le vecteur $e = -vi + uj$ est un vecteur directeur de $\mathcal{D}$ et le vecteur $e' = -v'i + u'j$ est un vecteur directeur de $\mathcal{D}'$. Les droites $\mathcal{D}$ et $\mathcal{D}'$ sont parallèles si et seulement si $e'$ est colinéaire à $e$. On a donc

$$\mathcal{D} \parallel \mathcal{D}' \iff \begin{vmatrix} u & v \\ u' & v' \end{vmatrix} = 0.$$

Si $A$ est le point de coordonnées $a, b$, la droite parallèle à $\mathcal{D}$ et passant par $A$ a pour équation $u(x-a) + v(y-b) = 0$. En effet, cette équation est celle d'une droite passant par $A$ et de vecteur directeur $-vi + uj = e$.

**Proposition.** *Soit $\mathscr{D}$ la droite d'équation $ux + vy + w = 0$ et soit $\mathscr{D}'$ la droite d'équation $u'x + v'y + w' = 0$. Supposons les droites $\mathscr{D}$ et $\mathscr{D}'$ sécantes. La droite $\mathscr{D}''$ d'équation $u''x + v''y + w'' = 0$ passe par le point d'intersection de $\mathscr{D}$ et $\mathscr{D}'$ si et seulement si on a*

$$\begin{vmatrix} u & v & w \\ u' & v' & w' \\ u'' & v'' & w'' \end{vmatrix} = 0.$$

**Démonstration.** Notons $a, b$ les coordonnées du point d'intersection de $\mathscr{D}$ et $\mathscr{D}'$. Supposons que la droite $\mathscr{D}''$ passe par ce point. Alors nous avons

$$\begin{cases} ua + vb + w = 0 \\ u'a + v'b + w' = 0 \\ u''a + v''b + w'' = 0 \end{cases}$$

c'est-à-dire

$$\begin{bmatrix} w \\ w' \\ w'' \end{bmatrix} = -a \begin{bmatrix} u \\ u' \\ u'' \end{bmatrix} - b \begin{bmatrix} v \\ v' \\ v'' \end{bmatrix}.$$

Dans le déterminant figurant dans la proposition, la troisième colonne est combinaison linéaire des deux premières, donc ce déterminant est égal à 0.

Réciproquement, supposons que le déterminant est nul. Puisque les droites $\mathscr{D}$ et $\mathscr{D}'$ ne sont pas parallèles, le déterminant $\begin{vmatrix} u & v \\ u' & v' \end{vmatrix}$ n'est pas nul, donc les vecteurs $(u, v)$ et $(u', v')$ sont linéairement indépendants. *A fortiori*, les vecteurs $(u, v, w)$ et $(u', v', w')$ sont aussi linéairement indépendants. Puisqu'on a $\begin{vmatrix} u & v & w \\ u' & v' & w' \\ u'' & v'' & w'' \end{vmatrix} = 0$, on en déduit que le vecteur $(u'', v'', w'')$ est combinaison linéaire de $(u, v, w)$ et $(u', v', w')$, autrement dit il existe des nombres réels $\lambda$, $\mu$ tels que

$$\begin{bmatrix} u'' \\ v'' \\ w'' \end{bmatrix} = \lambda \begin{bmatrix} u \\ v \\ w \end{bmatrix} + \mu \begin{bmatrix} u' \\ v' \\ w' \end{bmatrix}.$$

On a

$$\begin{aligned} u''a + v''b + w'' &= (\lambda u + \mu u')a + (\lambda v + \mu v')b + (\lambda w + \mu w') \\ &= \lambda(ua + vb + w) + \mu(u'a + v'b + w') = 0 \end{aligned}$$

car $ua + vb + w = 0$ et $u'a + v'b + w' = 0$ par hypothèse. L'égalité $u''a + v''b + w'' = 0$ signifie que la droite $\mathscr{D}''$ passe par le point de coordonnées $a, b$. ∎

Trois droites affines de $\mathbb{R}^2$ sont dites *concourantes* si elles ont exactement un point en commun.





**Exercice.** Soient $\mathscr{D}$ et $\mathscr{D}'$ des droites de $\mathbb{R}^2$ sécantes en un point $S$. Soient $A, B, C$ des points de $\mathscr{D}$, deux-à-deux différents et différents de $S$. Soient $A', B'$ des points de $\mathscr{D}'$, différents et différents de $S$. Notons $\mathscr{D}'_1$ la parallèle à $\mathscr{D}'$ passant par $A$ et $\mathscr{D}'_2$ la parallèle à $\mathscr{D}'$ passant par $B$.

a) Montrer que les droites $(CA')$, $(AB')$ et $(BA')$ sont bien définies.

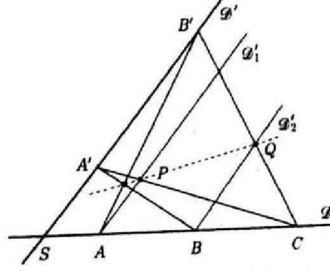
b) Montrer que la droite $(CA')$ coupe $\mathscr{D}'_1$ en un point $P$, que la droite $(CB')$ coupe $\mathscr{D}'_2$ en un point $Q$ et que l'on a $P \neq Q$.

c) On suppose que les droites $(AB')$ et $(BA')$ ne sont pas parallèles. Montrer que les droites $(PQ)$, $(AB')$ et $(BA')$ sont concourantes.

**Réponse**

a) On a $C \in \mathscr{D}$ et $C \neq S$, par suite $C \notin \mathscr{D}'$, car $S$ est le seul point qui appartient à la fois à la droite $\mathscr{D}$ et à la droite $\mathscr{D}'$. Puisque $A' \in \mathscr{D}'$, il vient $C \neq A'$. La droite $(CA')$ est donc bien définie. On démontre de même que les droites $(AB')$ et $(BA')$ sont bien définies.

b) Les droites $(CA')$ et $\mathscr{D}'$ sont sécantes en $A'$ donc elles ne sont pas parallèles. Par suite, $(CA')$ et $\mathscr{D}'_1$ ne sont pas non plus parallèles, autrement dit le point $P$ est bien défini. De même, les points $C$ et $B'$ sont différents et la droite $(CB')$ n'est pas parallèle à $\mathscr{D}'$, donc le point $Q$ est bien défini. Les droites parallèles $\mathscr{D}'_1$ et $\mathscr{D}'_2$ ne sont pas égales car $A \neq B$. Leur intersection est donc l'ensemble vide, par suite $P$ est différent de $Q$.




c) Puisque les droites $(SA)$ et $(SA')$ sont sécantes en $S$, les vecteurs $\overrightarrow{SA}$ et $\overrightarrow{SA'}$ sont linéairement indépendants. Choisissons $(S; \overrightarrow{SA}, \overrightarrow{SA'})$ comme repère cartésien de $\mathbb{R}^2$ et cherchons des équations des droites $(AB')$, $(BA')$ et $(PQ)$ dans ce repère. Les coordonnées de $A$ sont $1, 0$. Puisque $B'$ appartient à la droite $(SA')$ et est différent de $S$ et $A'$, la première coordonnée de $B'$ est nulle et la seconde est égale à $b'$ avec $b' \neq 0$ et $b' \neq 1$. Une équation de la droite $(AB')$ est donc

$$\begin{vmatrix} x - 1 & -1 \\ y & b' \end{vmatrix} = 0, \quad \text{c'est-à-dire} \quad b'x + y - b' = 0.$$

De même, les coordonnées de $A'$ sont $0, 1$ et celles de $B$ sont de la forme $b, 0$ avec $b \neq 0$ et $b \neq 1$. Une équation de la droite $(BA')$ est donc

$$\begin{vmatrix} x - b & -b \\ y & 1 \end{vmatrix} = 0, \quad \text{c'est-à-dire} \quad x + by - b = 0.$$

Cherchons maintenant les coordonnées des points $P$ et $Q$. Les coordonnées de $C$ sont de la forme $c, 0$ avec $c \neq 0$, $c \neq 1$ et $c \neq b$. Une équation de la droite $(CA')$ est $\begin{vmatrix} x-c & -c \\ y & 1 \end{vmatrix} = 0$, c'est-à-dire $x + cy - c = 0$. Puisque la droite $\mathscr{D}'_1$ a pour équation $x - 1 = 0$, les coordonnées de $P$ sont les nombres réels $x, y$ tels que $\begin{cases} x - 1 = 0 \\ x + cy - c = 0 \end{cases}$, c'est-à-dire sont $1, (c-1)/c$. De même, la droite $\mathscr{D}'_2$ a pour équation $x - b = 0$ et la droite $(CB')$ a pour équation $\begin{vmatrix} x-c & -c \\ y & b' \end{vmatrix} = 0$, c'est-à-dire $b'x + cy - b'c = 0$, donc les coordonnées de $Q$ sont $b, b'(c-b)/c$.
Il s'ensuit que la droite $(PQ)$ a pour équation

$$\begin{vmatrix} x-1 & b-1 \\ y-(c-1)/c & (b'(c-b)/c)-(c-1)/c \end{vmatrix} = 0,$$

c'est-à-dire $(b'(c-b) - c + 1)x - c(b-1)y - b'(c-b) + b(c-1) = 0$.
Calculons le déterminant

$$\Delta = \begin{vmatrix} b'(c-b)-c+1 & -c(b-1) & -b'(c-b)+b(c-1) \\ 1 & b & -b \\ b' & 1 & -b' \end{vmatrix}.$$

En ajoutant la troisième colonne à la première et à la deuxième, il vient

$$\Delta = \begin{vmatrix} (b-1)(c-1) & (c-b)(1-b') & -b'(c-b)+b(c-1) \\ 1-b & 0 & -b \\ 0 & 1-b' & -b' \end{vmatrix}$$

$$= (1-b')\begin{vmatrix} (b-1)(c-1) & c-b & -b'(c-b)+b(c-1) \\ 1-b & 0 & -b \\ 0 & 1 & -b' \end{vmatrix}.$$

Ajoutons $(b-c)$ fois la troisième ligne à la première. On obtient

$$\Delta = \begin{vmatrix} (b-1)(c-1) & 0 & b(c-1) \\ 1-b & 0 & -b \\ 0 & 1-b' & -b' \end{vmatrix}$$

$$= (1-b')\big(-b(b-1)(c-1) + b(c-1)(b-1)\big) = 0.$$

Puisque les droites $(AB')$ et $(BA')$ ne sont pas parallèles, elles sont sécantes. Puisque $\Delta = 0$, la droite $(PQ)$ passe par le point d'intersection des droites $(AB')$ et $(BA')$. Il s'ensuit que les droites $(AB')$, $(BA')$ et $(PQ)$ sont concourantes.

## 5. Géométrie affine dans l'espace

Les sous-espaces vectoriels de $\mathbb{R}^3$ sont de dimension 0, 1, 2 ou 3. Les sous-espaces affines sont donc

- les parties $\{A\}$ à un élément (dimension 0),
- les droites (dimension 1),
- les plans (dimension 2),
- l'espace $\mathbb{R}^3$ tout entier.



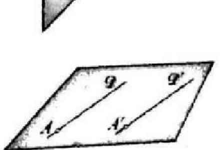
**Proposition.** *Deux plans de $\mathbb{R}^3$ non parallèles ont pour intersection une droite.*
*Soient $\mathscr{D}$ une droite et $\mathscr{P}$ un plan de $\mathbb{R}^3$. Si la direction de $\mathscr{D}$ n'est pas contenue dans la direction de $\mathscr{P}$, alors il existe un point $A$ tel que $\mathscr{D} \cap \mathscr{P} = \{A\}$.*

**Démonstration.** Soient $\mathscr{P}$ et $\mathscr{P}'$ des plans non parallèles. Leurs directions $P$ et $P'$ sont donc des sous-espaces vectoriels de $\mathbb{R}^3$, de dimension 2, tels que $P \neq P'$. Au chapitre 6 paragraphe 4, nous avons démontré l'égalité $\dim(P+P') = \dim P + \dim P' - \dim(P \cap P')$. Puisque $P+P'$ est un sous-espace vectoriel de $\mathbb{R}^3$, nous avons $\dim(P+P') \leqslant 3$ donc $\dim(P \cap P') = 2+2-\dim(P+P') \geqslant 4-3 = 1$. Par ailleurs, $P \cap P'$ est un sous-espace vectoriel de $P$ donc $\dim(P \cap P') \leqslant 2$. Puisque $P \neq P'$, on a $P \cap P' \neq P$ et par conséquent $\dim(P \cap P') = 1$. Il vient $\dim(P+P') = 2+2-1 = 3$ et par suite $P + P' = \mathbb{R}^3$. D'après une proposition page 161, il en résulte que l'intersection $\mathscr{P} \cap \mathscr{P}'$ n'est pas vide. Choisissons un point $A$ appartenant à $\mathscr{P}$ et à $\mathscr{P}'$. L'intersection $\mathscr{P} \cap \mathscr{P}'$ est le sous-espace affine passant par $A$ et de direction $P \cap P'$, c'est donc une droite.

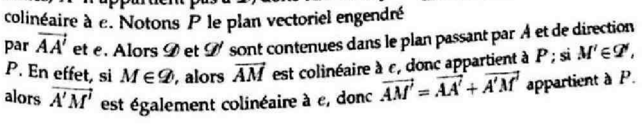
Démontrons la seconde affirmation. Notons $D$ la direction de $\mathscr{D}$ et $P$ celle de $\mathscr{P}$. Puisque $D$ n'est pas contenue dans $P$, il existe $e \in D$ tel que $e \notin P$. En particulier, $e$ n'est pas le vecteur nul. Choisissons une base $(f_1, f_2)$ de $P$. Puisque $e \notin P$, $e$ n'est pas combinaison linéaire de $f_1$ et $f_2$, donc $(e, f_1, f_2)$ est une base de $\mathbb{R}^3$. On a donc $\mathbb{R}^3 = D \oplus P$ : les sous-espaces vectoriels $D$ et $P$ sont supplémentaires. Comme nous l'avons montré au paragraphe 2, il s'ensuit que les sous-espaces affines $\mathscr{D}$ et $\mathscr{P}$ ont exactement un point en commun. ■

**Remarques**

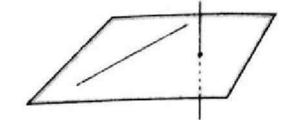
- Supposons que $\mathscr{D}$ et $\mathscr{D}'$ sont des droites différentes de $\mathbb{R}^3$ passant par un même point $A$. Les droites $\mathscr{D}$ et $\mathscr{D}'$ ne sont pas parallèles. Il existe donc un unique sous-espace vectoriel $P$ de dimension 2 de $\mathbb{R}^3$, contenant la direction de $\mathscr{D}$ et celle de $\mathscr{D}'$. Alors $\mathscr{D}$ et $\mathscr{D}'$ sont contenues dans le plan passant par $A$ et de direction $P$.




- Soient $\mathscr{D}, \mathscr{D}'$ des droites parallèles de $\mathbb{R}^3$ telles que $\mathscr{D} \neq \mathscr{D}'$.
  Choisissons un vecteur directeur $e$ de $\mathscr{D}$ et des points $A \in \mathscr{D}$ et $A' \in \mathscr{D}'$. Puisque $\mathscr{D}$ et $\mathscr{D}'$ sont différentes, $A'$ n'appartient pas à $\mathscr{D}$, donc $\overrightarrow{AA'}$ n'est pas colinéaire à $e$. Notons $P$ le plan vectoriel engendré par $\overrightarrow{AA'}$ et $e$. Alors $\mathscr{D}$ et $\mathscr{D}'$ sont contenues dans le plan passant par $A$ et de direction $P$. En effet, si $M \in \mathscr{D}$, alors $\overrightarrow{AM}$ est colinéaire à $e$, donc appartient à $P$ ; si $M' \in \mathscr{D}'$, alors $\overrightarrow{A'M'}$ est également colinéaire à $e$, donc $\overrightarrow{AM'} = \overrightarrow{AA'} + \overrightarrow{A'M'}$ appartient à $P$.



– En général, deux droites non parallèles de $\mathbb{R}^3$ ne se coupent pas.



Choisissons maintenant un repère cartésien $(O;i,j,k)$ de $\mathbb{R}^3$. Les points ont leurs coordonnées dans ce repère et les vecteurs ont leurs coordonnées dans la base $(i,j,k)$ de $\mathbb{R}^3$.

## Équation d'un plan

Soit $A$ le point de $\mathbb{R}^3$ de coordonnées $a,b,c$, c'est-à-dire $A = O + ai + bj + ck$. Soient $e_1 = r_1 i + s_1 j + t_1 k$ et $e_2 = r_2 i + s_2 j + t_2 k$ des vecteurs linéairement indépendants. Notons $\mathscr{P}$ le plan passant par $A$ et de direction le plan vectoriel $P$ engendré par $e_1$ et $e_2$. Pour tout point $M$ de coordonnées $x, y, z$, nous avons $M = O + xi + yj + zk$ donc

$$\overrightarrow{AM} = M - A = xi + yj + zk - ai - bj - ck = (x-a)i + (y-b)j + (z-c)k.$$

On en déduit les équivalences

$$M \in \mathscr{P} \iff \overrightarrow{AM} \text{ est combinaison linéaire de } e_1 \text{ et } e_2$$

$$\iff \begin{vmatrix} x-a & r_1 & r_2 \\ y-b & s_1 & s_2 \\ z-c & t_1 & t_2 \end{vmatrix} = 0.$$

Nous venons d'écrire une équation du plan passant par $A$ et de direction $P$. En développant le déterminant, cette équation prend la forme $ux + vy + wz + h = 0$ où les nombres $u, v, w$ ne sont pas tous nuls.

> Les plans affines de $\mathbb{R}^3$ ont pour équation $ux + vy + wz + h = 0$, où les nombres $u, v, w$ ne sont pas tous nuls.
> La direction du plan affine d'équation $ux + vy + wz + h = 0$ est le plan vectoriel d'équation $ux + vy + wz = 0$.

## Plans parallèles

Soit $\mathscr{P}$ le plan d'équation $ux + vy + wz + h = 0$ et soit $A$ le point de coordonnées $a, b, c$. Le plan parallèle à $\mathscr{P}$ et passant par $A$ a pour équation

$$u(x-a) + v(y-b) + w(z-c) = 0.$$



En effet, l'équation $u(x-a) + v(y-b) + w(z-c) = 0$ est celle d'un plan $\mathscr{P}'$ et puisque l'équation est vérifiée lorsque $(x,y,z) = (a,b,c)$, le plan $\mathscr{P}'$ passe par $A$. Montrons que $\mathscr{P}$ et $\mathscr{P}'$ sont parallèles. Choisissons un point $M_0$ appartenant à $\mathscr{P}$, de coordonnées $x_0, y_0, z_0$. Pour tout point $M' \in \mathscr{P}'$, de coordonnées $x', y', z'$, posons $M = M_0 + M' - A$. Les coordonnées de $M$ sont $x_0 + x' - a, y_0 + y' - b, z_0 + z' - c$ et l'on a

$$\begin{aligned} u(x_0 + x' - a) + v(y_0 + y' - b) + w(z_0 + z' - c) + h \\ = (ux_0 + vy_0 + wz_0 + h) + u(x'-a) + v(y'-a) + w(z'-a) = 0 \end{aligned}$$

car les coordonnées de $M'$ vérifient l'équation de $\mathscr{P}'$ et celles de $M_0$ l'équation de $\mathscr{P}$. Les coordonnées de $M$ vérifient donc l'équation de $\mathscr{P}$, autrement dit $M$ appartient à $\mathscr{P}$. Par suite le vecteur $\overrightarrow{M_0M}$ appartient à la direction de $\mathscr{P}$. Puisque $\overrightarrow{M_0M} = \overrightarrow{AM'}$, nous venons de démontrer que pour tout point $M' \in \mathscr{P}'$, le vecteur $\overrightarrow{AM'}$ appartient à la direction de $\mathscr{P}$. Cela signifie que le plan $\mathscr{P}'$ est parallèle à $\mathscr{P}$.

## Équations d'une droite

Soient $A$ un point de $\mathbb{R}^3$ et $e$ un vecteur non nul de $\mathbb{R}^3$. Notons $\mathscr{D}$ la droite de $\mathbb{R}^3$ passant par $A$ et de vecteur directeur $e$. Pour trouver des équations de $\mathscr{D}$, cherchons deux plans $\mathscr{P}_1$ et $\mathscr{P}_2$ non parallèles et contenant $\mathscr{D}$ : nous aurons alors $\mathscr{D} = \mathscr{P}_1 \cap \mathscr{P}_2$ d'après la proposition précédente.

Expliquons les calculs sur un exemple.

Supposons que les coordonnées de $A$ sont $0, 1, 2$ et que $e = 2i + j + 3k$. Alors $(e, i, j)$ est une base de $\mathbb{R}^3$ car le déterminant $\begin{vmatrix} 2 & 1 & 0 \\ 1 & 0 & 1 \\ 3 & 0 & 0 \end{vmatrix}$ est différent de 0. Notons $\mathscr{P}_1$ le plan passant par $A$ et de direction le plan vectoriel engendré par $e$ et $i$ et $\mathscr{P}_2$ le plan passant par $A$ et de direction le plan vectoriel engendré par $e$ et $j$. Ces plans ne sont pas parallèles et ils contiennent $\mathscr{D}$, par suite $\mathscr{D} = \mathscr{P}_1 \cap \mathscr{P}_2$. Une équation de $\mathscr{P}_1$ est

$$\begin{vmatrix} x & 2 & 1 \\ y-1 & 1 & 0 \\ z-2 & 3 & 0 \end{vmatrix} = 0, \quad \text{c'est-à-dire} \quad 3(y-1) - (z-2) = 0.$$

De même, une équation de $\mathscr{P}_2$ est

$$\begin{vmatrix} x & 2 & 0 \\ y-1 & 1 & 1 \\ z-2 & 3 & 0 \end{vmatrix} = 0 \quad \text{c'est-à-dire} \quad -3x + 2(z-2) = 0.$$

Des équations de $\mathscr{D}$ sont donc $\begin{cases} 3y - z - 1 = 0 \\ -3x + 2z - 4 = 0 \end{cases}$. La direction de $\mathscr{D}$ est la droite vectorielle d'équation $\begin{cases} 3y - z = 0 \\ -3x + 2z = 0 \end{cases}$.

Une droite de $\mathbb{R}^3$ est ainsi déterminée par deux équations de plans.

# 6. Applications affines

Dans ce paragraphe, $n$ et $p$ sont des entiers positifs.

**Définition**

Soit $f : \mathbb{R}^p \to \mathbb{R}^n$ une application. On dit que $f$ est une *application affine* s'il existe une application linéaire $g : \mathbb{R}^p \to \mathbb{R}^n$ et un vecteur $u \in \mathbb{R}^n$ tels que

$$f(M) = g(M) + u \quad \text{pour tout } M \in \mathbb{R}^p.$$

Pour tous points $P$ et $Q$ de $\mathbb{R}^n$, nous avons

$$f(Q) - f(P) = \big(g(Q) + u\big) - \big(g(P) + u\big) = g(Q) - g(P) = g(Q - P)$$

car l'application $g$ est linéaire. On a donc $\overrightarrow{f(P)f(Q)} = g(\overrightarrow{PQ})$.

Notons $\mathbf{A}$ la matrice de l'application linéaire $g$ dans les bases canoniques de $\mathbb{R}^p$ et $\mathbb{R}^n$ et posons $u = (u_1, \ldots, u_n)$. Pour tout point $M = (x_1, \ldots, x_p)$ appartenant à $\mathbb{R}^p$, le point $f(M) = (y_1, \ldots, y_n)$ se calcule en utilisant l'égalité matricielle

$$\begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = \mathbf{A} \begin{bmatrix} x_1 \\ \vdots \\ x_p \end{bmatrix} + \begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix}.$$

**Exemples**

- Soit $f : \mathbb{R}^2 \to \mathbb{R}$ une application affine. Par définition, il existe une application linéaire $g : \mathbb{R}^2 \to \mathbb{R}$ et un nombre réel $u$ tel que $f(x,y) = g(x,y) + u$ pour tous $x, y \in \mathbb{R}$. Puisque $g$ est une forme linéaire sur $\mathbb{R}^2$, il existe des nombres réels $a$ et $b$ tels que $g(x,y) = ax + by$ pour tous $x, y \in \mathbb{R}$. On a donc $f(x,y) = ax + by + u$ pour tous $x, y \in \mathbb{R}$.
- Soient $g : \mathbb{R}^2 \to \mathbb{R}^2$ une application linéaire et $(r,s) \in \mathbb{R}^2$. Puisque la matrice de $g$ est de la forme $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, l'application affine $f : \mathbb{R}^2 \to \mathbb{R}^2$ définie par $f(x,y) = g(x,y) + (r,s)$ s'explicite de la manière suivante. Si $f(x,y) = (x', y')$, alors

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} r \\ s \end{bmatrix} = \begin{bmatrix} ax + by \\ cx + dy \end{bmatrix} + \begin{bmatrix} r \\ s \end{bmatrix} = \begin{bmatrix} ax + by + r \\ cx + dy + s \end{bmatrix}$$

autrement dit, nous avons $f(x,y) = (ax + by + r, cx + dy + s)$ pour tous $x, y \in \mathbb{R}$.

Voici des propriétés générales des applications affines.

**Proposition.** *Soient $g : \mathbb{R}^p \to \mathbb{R}^n$ une application linéaire, $u$ un vecteur de $\mathbb{R}^n$ et $f : \mathbb{R}^p \to \mathbb{R}^n$ l'application affine définie par $f(M) = g(M) + u$ pour tout $M \in \mathbb{R}^p$. S'il existe un point $A \in \mathbb{R}^p$ tel que $f(A) = 0$, alors l'ensemble $\{ M \in \mathbb{R}^p \mid f(M) = 0 \}$ est le sous-espace affine de $\mathbb{R}^p$ passant par $A$ et de direction $\operatorname{Ker} g$.*





**Démonstration.** Posons $\mathscr{V} = \{ M \in \mathbb{R}^p \mid f(M) = 0 \}$. Puisque $f(A) = 0$, le point $A$ appartient à $\mathscr{V}$. Pour tout point $M \in \mathbb{R}^p$, on a les équivalences

$$\begin{aligned} M \in \mathscr{V} &\iff f(M) = 0 \iff f(M) = f(A) \\ &\iff \overrightarrow{f(A)f(M)} = 0 \iff g(\overrightarrow{AM}) = 0 \iff \overrightarrow{AM} \in \operatorname{Ker} g \end{aligned}$$

d'où le résultat. ∎

**Exemples**

- Soient $u, v$ des nombres réels non tous deux nuls et soit $w \in \mathbb{R}$. Considérons l'application affine $f : \mathbb{R}^2 \to \mathbb{R}$ définie par $f(x,y) = ux + vy + w$. Si $u$ n'est pas nul, alors $f(-w/u, 0) = 0$ et si $v$ n'est pas nul, alors $f(0, -w/v) = 0$. Dans tous les cas, il existe un point $A \in \mathbb{R}^2$ tel que $f(A) = 0$. Par définition, le noyau de l'application linéaire $g : \mathbb{R}^2 \to \mathbb{R}$ définie par $g(x,y) = ux + vy$, est la droite vectorielle $D$ d'équation $ux + vy = 0$. La droite affine d'équation $ux + vy + w = 0$ passe par $A$ et a pour direction $D$.
- De même, considérons le système d'équations $\begin{cases} ux + vy + wz + h = 0 \\ u'x + v'y + w'z + h' = 0 \end{cases}$ à coefficients réels. Supposons que ce système d'équations a une solution $A = (x_0, y_0, z_0)$. Alors l'ensemble des solutions est un sous-espace affine de $\mathbb{R}^3$ passant par le point $A$. La direction est le noyau de l'application linéaire $g : \mathbb{R}^3 \to \mathbb{R}^2$ définie par $g(x,y,z) = (ux + vy + wz, u'x + v'y + w'z)$, c'est-à-dire l'ensemble des solutions du système d'équations $\begin{cases} ux + vy + wz = 0 \\ u'x + v'y + w'z = 0. \end{cases}$

**Proposition.** *Soient $k$ un entier positif, $A_1, \ldots, A_k$ des points de $\mathbb{R}^p$ et $a_1, \ldots, a_k$ des nombres réels tels que $a_1 + \cdots + a_k \neq 0$. Soit $G$ le barycentre des points $A_1, \ldots, A_k$ affectés des coefficients $a_1, \ldots, a_k$. Si $f$ est une application affine de $\mathbb{R}^p$ dans $\mathbb{R}^n$, alors $f(G)$ est le barycentre des points $f(A_1), \ldots, f(A_k)$ affectés des coefficients $a_1, \ldots, a_k$.*

**Démonstration.** L'application $f$ est définie par $f(M) = g(M) + u$, où $g : \mathbb{R}^p \to \mathbb{R}^n$ est une application linéaire et $u \in \mathbb{R}^n$. En posant $s = a_1 + \cdots + a_k$, nous avons par définition $G = \frac{1}{s}(a_1 A_1 + \cdots + a_k A_k)$ donc

$$\begin{aligned} f(G) = g(G) + u &= \frac{1}{a_1 + \cdots + a_k}\Big(a_1 g(A_1) + \cdots + a_k g(A_k)\Big) + u \\ &= \frac{1}{s}\Big(a_1 g(A_1) + \cdots + a_k g(A_k) + a_1 u + \cdots + a_k u\Big) \\ &= \frac{1}{s}\Big(a_1\big(g(A_1) + u\big) + \cdots + a_k\big(g(A_k) + u\big)\Big) \\ &= \frac{1}{s}\Big(a_1 f(A_1) + \cdots + a_k f(A_k)\Big). \end{aligned}$$

∎

En particulier, une application affine $f$ transforme isobarycentre en isobarycentre. Par exemple, si $I$ est le milieu de $AB$, alors $f(I)$ est le milieu de $f(A)f(B)$.

Terminons le chapitre en étudiant quelques applications affines importantes en géométrie.

## Projections

Soient $F$ et $G$ des sous-espaces vectoriels de $\mathbb{R}^n$ tels que $F \oplus G = \mathbb{R}^n$, $F \neq \{0\}$ et $G \neq \{0\}$. Rappelons que nous avons défini au chapitre **7** la projection sur $F$ parallèlement à $G$ : c'est l'application linéaire $p' : \mathbb{R}^n \to \mathbb{R}^n$ telle que $p'(x+y) = x$ quels que soient $x \in F$ et $y \in G$.

Soient $A$ un point de $\mathbb{R}^n$ et $\mathcal{F}$ le sous-espace affine passant par $A$ et de direction $F$.

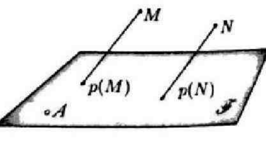
**Définition**

La *projection sur* $\mathcal{F}$ *parallèlement à* $G$ est l'application $p : \mathbb{R}^n \to \mathbb{R}^n$ définie par $p(M) = A + p'(M - A)$.

Si $B$ est un point de $\mathcal{F}$, nous avons $B - A \in F$ donc $B - A = p'(B-A) = p'(B) - p'(A)$ ou encore $B - p'(B) = A - p'(A)$. Pour tout $M \in \mathbb{R}^n$, il vient $A + p'(M - A) = A + p'(M) - p'(A) = B + p'(M) - p'(B) = B + p'(M - B)$. L'application $p$ que nous venons de définir ne dépend donc pas du choix du point $A \in \mathcal{F}$.

**Proposition.** *La projection $p$ est une application affine. Si $M \in \mathcal{F}$, alors $p(M) = M$. Pour tout $M \in \mathbb{R}^n$, on a $p(M) \in \mathcal{F}$, $\overrightarrow{Mp(M)} \in G$ et $p(p(M)) = p(M)$.*

**Démonstration.** Puisque $p'$ est une application linéaire, nous avons $p(M) = p'(M) + A - p'(A)$ pour tout $M \in \mathbb{R}^n$. L'application $p$ est donc affine. L'image de $p'$ est $F$, donc $p'(M - A) \in F$ pour tout point $M \in \mathbb{R}^n$. Puisque $A \in \mathcal{F}$, on en déduit $p(M) \in \mathcal{F}$. Si $M \in \mathcal{F}$, alors $M - A \in F$, par suite $p'(M - A) = M - A$ et $p(M) = A + M - A = M$. Pour tout vecteur $u \in \mathbb{R}^n$, on a $p'(u) - u \in G$ : en effet, nous avons $u = x + y$ où $x \in F$ et $y \in G$ et il vient $p'(u) - u = p'(x+y) - (x+y) = x - (x+y) = -y$. Pour tout point $M \in \mathbb{R}^n$, on a $\overrightarrow{Mp(M)} = p(M) - M = p'(M - A) - (M - A)$ donc $\overrightarrow{Mp(M)} \in G$. Enfin, puisque $p(M) \in \mathcal{F}$ pour tout $M$, on a $p(p(M)) = p(M)$. ∎








## Symétries

Gardons les notations introduites ci-dessus. Comme nous l'avons défini au chapitre 7, la symétrie par rapport à $F$ parallèlement à $G$ est l'application linéaire $s' : \mathbb{R}^n \to \mathbb{R}^n$ définie par $s'(x + y) = x - y$ quels que soient $x \in F$ et $y \in G$.

**Définition**

La *symétrie par rapport à* $\mathcal{F}$ *parallèlement à* $G$ est l'application $s : \mathbb{R}^n \to \mathbb{R}^n$ définie par $s(M) = A + s'(M - A)$.

On montre comme pour une projection, que l'application $s$ ne dépend pas du choix du point $A \in \mathcal{F}$.

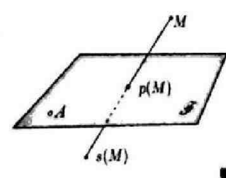
**Proposition.** *La symétrie $s$ est une application affine. Pour tout point $M \in \mathbb{R}^n$, on a $(M \in \mathcal{F} \Leftrightarrow s(M) = M)$, $\overrightarrow{Ms(M)} \in G$ et $s(s(M)) = M$. De plus, le milieu de $Ms(M)$ est un point de $\mathcal{F}$.*

**Démonstration.** L'application $s'$ est linéaire et l'on a $s(M) = s'(M) + A - s(A)$ pour tout point $M \in \mathbb{R}^n$. L'application $s$ est donc affine. Pour tout vecteur $u \in \mathbb{R}^n$, nous avons l'équivalence $u \in F \Leftrightarrow s'(u) = u$. Puisque $A$ est un point de $\mathcal{F}$, on en déduit les équivalences

$$M \in \mathcal{F} \iff M - A \in F \iff s'(M - A) = M - A \iff s(M) = M.$$

Pour tout vecteur $u \in \mathbb{R}^n$, on a $s'(u) - u \in G$. Puisque $s(M) - M = s'(M - A) - (M - A)$, on en déduit que $s(M) - M \in G$.

On a $s(s(M)) = A + s'(s(M) - A) = A + s'(s'(M - A))$. Or pour tout vecteur $u \in \mathbb{R}^n$, on a $s'(s'(u)) = u$, donc il vient $s(s(M)) = A + (M - A) = M$. Soient $M \in \mathbb{R}^n$ et $I$ le milieu de $Ms(M)$. Puisque $s$ est une application affine, le point $s(I)$ est le milieu de $s(M)s(s(M))$, c'est-à-dire le milieu de $s(M)M$. On a donc $s(I) = I$ et par suite $I \in \mathcal{F}$. ∎




Le sous-espace affine $\mathcal{F}$ s'appelle le *sous-espace affine des points fixes de* $s$.

**Remarque**

Nous pouvons définir de la même manière la symétrie par rapport à $\mathcal{F}$ parallèlement à $G$, lorsque $F = \{0\}$ et $G = \mathbb{R}^n$. Dans ce cas, $\mathcal{F} = \{A\}$ et $s'(u) = -u$ quel que soit le vecteur $u \in \mathbb{R}^n$. Il vient donc $s(M) = 2A - M$ pour tout point $M \in \mathbb{R}^n$. On dit simplement que $s$ est la *symétrie par rapport à* $A$.

**Exercice.** Soit $f : \mathbb{R}^2 \to \mathbb{R}^2$ l'application affine définie par

$$f(x,y) = (7x + 24y + 3, -2x - 7y - 1) \quad \text{pour tous} \quad x, y \in \mathbb{R}.$$

Montrer que $f$ est une symétrie, en trouver la direction et le sous-espace affine des points fixes.

**Réponse.** Soit $g : \mathbb{R}^2 \to \mathbb{R}^2$ l'application linéaire définie par

$$g(x,y) = (7x + 24y, -2x - 7y) \quad \text{pour tous} \quad x, y \in \mathbb{R}.$$

Pour tous $x, y \in \mathbb{R}$, on a les équivalences

$$g(x,y) = (x,y) \iff \begin{cases} 6x + 24y = 0 \\ -2x - 8y = 0 \end{cases} \iff x + 4y = 0$$

$$g(x,y) = -(x,y) \iff \begin{cases} 8x + 24y = 0 \\ -2x - 6y = 0 \end{cases} \iff x + 3y = 0.$$

Notons $D$ la droite vectorielle d'équation $x + 4y = 0$ et $D'$ la droite vectorielle d'équation $x + 3y = 0$. La droite $D$ est engendrée par le vecteur $(-4, 1)$ et la droite $D'$ est engendrée par le vecteur $(-3, 1)$. Ces deux vecteurs ne sont pas colinéaires, donc les sous-espaces vectoriels $D$ et $D'$ de $\mathbb{R}^2$ sont supplémentaires. L'application linéaire $g$ est donc la symétrie par rapport à $D$ parallèlement à $D'$.

Pour tout point $(x,y) \in \mathbb{R}^2$, on a les équivalences

$$f(x,y) = (x,y) \iff \begin{cases} 6x + 24y = -3 \\ -2x - 8y = 1 \end{cases} \iff 2x + 8y + 1 = 0.$$

Les points $(x,y)$ tels que $f(x,y) = (x,y)$ sont donc ceux de la droite affine $\mathscr{D}$ d'équation $2x + 8y + 1 = 0$. Cette droite passe par le point $A = (-1/2, 0)$ et a pour direction $D$. Quel que soit le point $M = (x,y)$ appartenant à $\mathbb{R}^2$, nous avons

$$\begin{aligned} A + g(M - A) &= (-1/2, 0) + g(x + 1/2, y) \\ &= (-1/2, 0) + (7(x + 1/2) + 24y, -2(x + 1/2) - 7y) \\ &= (7x + 24y + 3, -2x - 7y - 1) = f(M) \end{aligned}$$

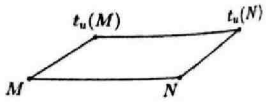
donc $f$ est la symétrie par rapport à $\mathscr{D}$ parallèlement à $D'$. De plus, le sous-espace affine des points fixes de $f$ est la droite $\mathscr{D}$.

## Translations

### Définition

Soit $u$ un vecteur de $\mathbb{R}^n$. La *translation de vecteur* $u$ est l'application affine $t_u : \mathbb{R}^n \to \mathbb{R}^n$ définie par $t_u(M) = M + u$.

On a $t_0 = \mathrm{id}_{\mathbb{R}^n}$ et si $u$ et $v$ sont des vecteurs de $\mathbb{R}^n$, alors $t_u \circ t_v = t_{u+v}$. De plus, une application $f : \mathbb{R}^n \to \mathbb{R}^n$ est une translation si et seulement si $\overrightarrow{f(P)f(Q)} = \overrightarrow{PQ}$ pour tous points $P, Q \in \mathbb{R}^n$.






## Homothéties

### Définition

Soit $k$ un nombre réel différent de 0 et 1 et soit $u$ un vecteur de $\mathbb{R}^n$. L'application affine $h : \mathbb{R}^n \to \mathbb{R}^n$ définie par $h(M) = kM + u$ s'appelle une *homothétie de rapport* $k$.

**Proposition.** *Soit $k$ un nombre réel différent de 0 et 1.*

- *Si $h : \mathbb{R}^n \to \mathbb{R}^n$ est une homothétie de rapport $k$, alors il existe un unique point $O \in \mathbb{R}^n$ tel que $h(O) = O$. De plus, on a $h(M) = O + k\overrightarrow{OM}$ pour tout point $M \in \mathbb{R}^n$.*
- *Une application $f : \mathbb{R}^n \to \mathbb{R}^n$ est une homothétie de rapport $k$ si et seulement si $\overrightarrow{f(P)f(Q)} = k\overrightarrow{PQ}$ quels que soient les points $P$ et $Q$ de $\mathbb{R}^n$.*

**Démonstration.** Soit $h$ une homothétie de rapport $k$. Par définition, il existe un vecteur $u \in \mathbb{R}^n$ tel que $h(M) = kM + u$ pour tout $M \in \mathbb{R}^n$. On a les équivalences

$$h(M) = M \iff (1 - k)M = u \iff M = \frac{1}{1-k}u.$$

Le point $O$ est donc $\frac{1}{1-k}u$. Pour tout point $M$, il vient

$$h(M) - O = h(M) - h(O) = (kM + u) - (kO + u) = k(M - O),$$

c'est-à-dire $h(M) = O + k\overrightarrow{OM}$.

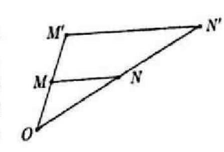
Si $f$ est l'homothétie définie par $f(M) = kM + u$, alors pour tous points $P, Q$, on a $\overrightarrow{f(P)f(Q)} = f(Q) - f(P) = (kQ + u) - (kP + u) = k(Q - P) = k\overrightarrow{PQ}$. Réciproquement, supposons que $f$ est une application de $\mathbb{R}^n$ dans $\mathbb{R}^n$ et que l'on a $\overrightarrow{f(P)f(Q)} = k\overrightarrow{PQ}$ quels que soient les points $P$ et $Q$. Choisissons un point $A$. Pour tout point $P$ de $\mathbb{R}^n$, nous avons $f(P) - f(A) = \overrightarrow{f(A)f(P)} = k\overrightarrow{AP} = kP - kA$ donc $f(P) = kP + u$, où l'on a posé $u = f(A) - kA$. L'application $f$ est donc une homothétie de rapport $k$. ∎

Il résulte de la proposition précédente que le nombre $k$ est unique et que l'image d'une droite par une homothétie est une droite parallèle.

### Définitions

Le point $O$ de la proposition précédente s'appelle le *centre* de l'homothétie $h$ et le scalaire $k$ s'appelle le *rapport* de l'homothétie.

Si $h$ est une homothétie de centre $O$, alors pour tout point $M$, les points $O$, $M$ et $h(M)$ sont alignés, d'après la proposition précédente. Si l'on connaît deux points différents $M$ et $N$ et leurs images $M' = h(M)$, $N' = h(N)$, le centre de $h$ est donc l'intersection des droites $(MM')$ et $(NN')$.



**Application : le théorème de Thalès.** Soient $\mathscr{D}_1$ et $\mathscr{D}_2$ deux droites de $\mathbb{R}^2$, sécantes en $O$. Soient $M$ et $M'$ des points de $\mathscr{D}_1$, différents et différents de $O$. De même, soient $N$ et $N'$ des points de $\mathscr{D}_2$, différents et différents de $O$. Alors les droites $(MN)$ et $(M'N')$ sont parallèles si et seulement si $\frac{\overline{OM'}}{\overline{OM}} = \frac{\overline{ON'}}{\overline{ON}}$.

En effet, posons $k = \frac{\overline{OM'}}{\overline{OM}}$ et notons $h$ l'homothétie de centre $O$ et de rapport $k$. Si l'on a $\frac{\overline{OM'}}{\overline{OM}} = \frac{\overline{ON'}}{\overline{ON}}$, alors il vient $\overrightarrow{ON'} = k\overrightarrow{ON}$ et donc $h(N) = N'$. Puisque $h(M) = M'$, les droites $(MN)$ et $(M'N')$ sont parallèles. Réciproquement, si les droites $(MN)$ et $(M'N')$ sont parallèles, alors $h(N)$ appartient à la parallèle à la droite $(MN)$ passant par $h(M)$, c'est-à-dire à la droite $(M'N')$. D'autre part, les points $O$, $N$ et $h(N)$ sont alignés, donc $h(N) \in (ON')$. Par suite on a $h(N) = N'$, d'où l'égalité des rapports.

Voici comment identifier la composée d'une homothétie et d'une translation, ou la composée de deux homothéties.

**Proposition.** *Soit $h$ une homothétie de rapport $k$.*

- *Si $t$ est une translation, alors les composées $h \circ t$ et $t \circ h$ sont des homothéties de même rapport $k$.*
- *Soit $h'$ une homothétie de rapport $k'$. Si $kk' \neq 1$, alors la composée $h \circ h'$ est une homothétie de rapport $kk'$ et les centres de $h$, $h'$ et $h \circ h'$ sont des points alignés. Si $kk' = 1$, alors la composée $h \circ h'$ est une translation.*

**Démonstration.** Si $t$ est la translation de vecteur $u$, alors pour tous points $P$ et $Q$ on a

$$\overrightarrow{h(t(P))h(t(Q))} = k\overrightarrow{t(P)t(Q)} = k\big((Q+u) - (P+u)\big) = k\overrightarrow{PQ}$$

et

$$\overrightarrow{t(h(P))t(h(Q))} = \overrightarrow{h(P)h(Q)} = k\overrightarrow{PQ}.$$

Les applications $h \circ t$ et $t \circ h$ sont donc des homothéties de rapport $k$.
Notons $O$ le centre de $h$ et $O'$ le centre de $h'$. Pour tout point $M \in \mathbb{R}^n$, nous avons $h(M) = O + k(M - O) = (1-k)O + kM$ et de même $h'(M) = (1-k')O' + k'M$, donc

$$\begin{aligned} h(h'(M)) = h\big((1-k')O' + k'M\big) &= (1-k)O + k\big((1-k')O + k'M)\big) \\ &= (1-k)O + k(1-k')O' + kk'M. \end{aligned}$$

Si $kk' \neq 1$, l'application $h \circ h'$ est donc une homothétie de rapport $kk'$. Le centre de $h \circ h'$ est le point $\Omega$ tel que

$$\begin{aligned} h \circ h'(\Omega) = \Omega &\iff (1-k)O + k(1-k')O' + kk'\Omega = \Omega \\ &\iff \Omega = \frac{1}{1-kk'}\big((1-k)O + k(1-k')O'\big). \end{aligned}$$





Puisque $1 - kk' = (1-k) + k(1-k')$, le point $\Omega$ est le barycentre des points $O$ et $O'$ affectés des coefficients $1-k$ et $k(1-k')$. Si $O \neq O'$, alors $\Omega$ appartient à la droite $(OO')$. Si $O = O'$, alors $\Omega = O$.

Si $kk' = 1$, alors pour tout point $M$ nous avons $h \circ h'(M) = M + u$ où $u = (1-k)O + k(1-k')O' = (k-1)\overrightarrow{OO'}$. L'application $h \circ h'$ est donc la translation de vecteur $u$.

■

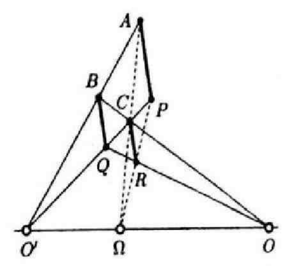
**Remarque**

Supposons que $h$ et $h'$ sont des homothéties de centres différents et que la composée $h \circ h'$ est une homothétie. Voici comment on peut démontrer géométriquement l'alignement des centres $O$, $O'$ et $\Omega$ de $h$, $h'$ et $h \circ h'$.

Puisque $O$ est le centre de $h$, les points $O$, $O'$ et $h(O')$ sont alignés. De même, le centre $\Omega$ de $h \circ h'$ est sur la droite passant par $O'$ et $h \circ h'(O')$. Puisqu'on a $h \circ h'(O') = h(O')$, le point $\Omega$ est sur la droite $(O'\,h(O'))$, c'est-à-dire sur la droite $(OO')$.

Sur cette figure, nous avons représenté

- les points $A$ et $P$ et leurs images $B = h'(A)$, $Q = h'(P)$ : les droites $(AP)$ et $(BQ)$ sont parallèles et les droites $(AB)$ et $(PQ)$ se coupent au centre $O'$ de l'homothétie $h'$ ;
- les points $C = h(B)$ et $R = h(Q)$ : les droites $(BQ)$ et $(CR)$ sont parallèles et les droites $(BC)$ et $(QR)$ se coupent au centre $O$ de l'homothétie $h$ ;




- le centre $\Omega$ de l'homothétie $h \circ h'$ : on a $(h \circ h')(A) = C$ et $(h \circ h')(P) = R$, de sorte que les droites $(AC)$ et $(PR)$ se coupent en $\Omega$.

## Exercices

Il faut dessiner une figure chaque fois que possible.

1. Soient $A, B, C, D$ des points de $\mathbb{R}^3$. On suppose qu'il n'existe pas de plan affine de $\mathbb{R}^3$ contenant $A, B, C, D$. Montrer que les points $A, B, C, D$ sont deux à deux différents et que $(A; \overrightarrow{AB}, \overrightarrow{AC}, \overrightarrow{AD})$ est un repère cartésien de $\mathbb{R}^3$.

2. Considérons les points de $\mathbb{R}^3$ : $A = (0,1,1)$, $B = (-2,0,1)$, $C = (1,1,3)$. Montrer qu'il existe un unique plan de $\mathbb{R}^3$ passant par $A, B, C$. Trouver une équation du plan $(ABC)$.

**3.** Soit $h : \mathbb{R}^3 \to \mathbb{R}^3$ l'application définie par $h(x, y, z) = (3 - 2x, -1 - 2y, 1 - 2z)$. Montrer que $h$ est une homothétie, trouver son centre et son rapport.

**4.** Soit $\mathscr{D}$ la droite de $\mathbb{R}^3$ d'équations $\begin{cases} 2x + y - z - 1 = 0 \\ x - z - 2 = 0 \end{cases}$ et soit $A = (1, 0, 0)$.

**a)** Trouver deux points différents $B$ et $C$ appartenant à $\mathscr{D}$.

**b)** Montrer qu'il existe un unique plan $\mathscr{P}$ de $\mathbb{R}^3$ passant par $A$ et contenant $\mathscr{D}$. Trouver une équation de $\mathscr{P}$.

**5.** Soit $\mathscr{P}$ le plan de $\mathbb{R}^3$ d'équation $x - y + z - 2 = 0$ et de direction $P$. Soit $D$ la droite vectorielle de $\mathbb{R}^3$ engendrée par le vecteur $u = (1, 0, 1)$.

**a)** Trouver une équation de $P$ et montrer que les sous-espaces vectoriels $D$ et $P$ de $\mathbb{R}^3$ sont supplémentaires.

**b)** Trouver une base $(e, f)$ de $P$. Calculer les coordonnées du vecteur $(x, y, z) \in \mathbb{R}^3$ dans la base $(e, f, u)$.

**c)** Trouver un point appartenant à $\mathscr{P}$. Soit $s$ la symétrie par rapport à $\mathscr{P}$ parallèlement à $D$. Calculer $s(x, y, z)$ pour tout $(x, y, z) \in \mathbb{R}^3$.

**d)** Soit $\mathscr{Q}$ le plan d'équation $x + z = 0$. Montrer que pour tout point $M \in \mathbb{R}^3$, on a l'équivalence $M \in s(\mathscr{Q}) \Leftrightarrow s(M) \in \mathscr{Q}$. Montrer que $s(\mathscr{Q})$ est un plan et trouver une équation de ce plan.

**6.** Soient $O, A, B, C$ des points de $\mathbb{R}^3$. On suppose que $A, B, C$ ne sont pas alignés et que $O$ n'appartient pas au plan $(ABC)$. Soit $\mathscr{P}$ un plan parallèle à $(ABC)$, différent du plan $(ABC)$ et ne passant pas par $O$.

**a)** Montrer qu'il existe des points $P, Q, R$ tels que $\mathscr{P} \cap (OA) = \{P\}$, $\mathscr{P} \cap (OB) = \{Q\}$ et $\mathscr{P} \cap (OC) = \{R\}$.

**b)** Posons $k = \dfrac{\overline{OP}}{\overline{OA}}$. Montrer que l'on a $k \neq 0$ et $k \neq 1$.

**c)** Soit $h$ l'homothétie de centre $O$ et de rapport $k$. Montrer que $h(A) = P$, $h(B) = Q$ et $h(C) = R$.

**d)** Soient $I$ le milieu de $BC$, $J$ le milieu de $AC$, $K$ le milieu de $AB$ et $G$ l'isobarycentre des points $A, B, C$. Montrer que les points $A, I, G$ sont alignés. Soit $h'$ l'homothétie de centre $G$ et de rapport $-2$. Montrer que $h'(I) = A$, $h'(J) = B$ et $h'(K) = C$.

**e)** Quels sont les points $h \circ h'(I)$, $h \circ h'(J)$, $h \circ h'(K)$ ? Montrer que les droites $(PI)$, $(QJ)$ et $(RK)$ sont concourantes si $k \neq -1/2$ et que ces droites sont parallèles si $k = -1/2$.



**7.** Soient $A, B, C$ des points non alignés de $\mathbb{R}^2$. On choisit $(A; \overrightarrow{AB}, \overrightarrow{AC})$ comme repère cartésien de $\mathbb{R}^2$. Soit $M$ un point de la droite $(BC)$.

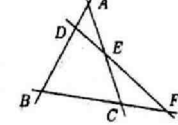
**a)** Montrer qu'il existe un unique point $M_1$ point d'intersection de la droite $(AC)$ et de la parallèle à $(AB)$ passant par $M$. Montrer qu'il existe un unique point $M_2$ point d'intersection de la droite $(AB)$ et de la parallèle à $(BC)$ passant par $M_1$. Montrer qu'il existe un unique point $M_3$ point d'intersection de $(BC)$ et de la parallèle à $(CA)$ passant par $M_2$.

**b)** Calculer les coordonnées des points $M_1, M_2, M_3$ au moyen des coordonnées de $M$.

**c)** Trouver une équation de la droite $(BC)$. Montrer que $M_3$ est le symétrique de $M$ par rapport au milieu de $BC$.

**d)** À partir du point $M_3$, on construit comme en (a) les points $M_4 \in (AC)$, $M_5 \in (AB)$ et $M_6 \in (BC)$. Montrer que l'on a $M = M_6$.

**8.** Considérons quatre droites de $\mathbb{R}^2$, chacune coupant les trois autres en trois points différents. Notons, comme sur la figure ci-contre, $A, B, C, D, E, F$ les points d'intersection obtenus et choisissons $(A; \overrightarrow{AB}, \overrightarrow{AC})$ comme repère cartésien de $\mathbb{R}^2$. Notons $q, 0$ les coordonnées de $D$ et $0, r$ celles de $E$.




**a)** Trouver une équation de la droite $(BC)$ et une équation de la droite $(DE)$.

**b)** Calculer les coordonnées de $F$ au moyen de $q$ et $r$.

**c)** Soient $I$ le milieu de $CD$, $J$ le milieu de $BE$ et $K$ le milieu de $AF$. Calculer les coordonnées de $I, J, K$. Montrer que les points $I, J, K$ sont alignés.

**9.** Soient $A, B, C$ des points non alignés de $\mathbb{R}^2$. On choisit $(A; \overrightarrow{AB}, \overrightarrow{AC})$ comme repère cartésien de $\mathbb{R}^2$. Soient $P \in (BC)$, $Q \in (CA)$ et $R \in (AB)$. On suppose que les points $P, Q, R$ sont tous différents des points $A, B, C$.

**a)** Soient $u, v$ les coordonnées de $P$. Montrer que $u$ et $v$ sont non nuls et que l'on a $u + v = 1$. Calculer $\dfrac{\overline{PC}}{\overline{PB}}$ au moyen de $u$.

**b)** Montrer que les coordonnées de $Q$ sont de la forme $0, q$ où $q$ est un nombre réel différent de 0 et 1. Calculer $\dfrac{\overline{QA}}{\overline{QC}}$ au moyen de $q$.

**c)** Montrer que les coordonnées de $R$ sont de la forme $r, 0$ où $r$ est un nombre réel différent de 0 et 1. Calculer $\dfrac{\overline{RB}}{\overline{RA}}$ au moyen de $r$.

**d)** Trouver des équations des droites $(AP)$, $(BQ)$ et $(CR)$ au moyen des nombres $u, q, r$.

**e)** On suppose que les droites $(AP)$ et $(BQ)$ sont sécantes. Montrer que les droites $(AP)$, $(BQ)$ et $(CR)$ sont concourantes si et seulement si $\frac{\overline{PC}}{\overline{PB}}\frac{\overline{QA}}{\overline{QC}}\frac{\overline{RB}}{\overline{RA}} = -1$.

**10.** Soient $A, B, C$ des points non alignés de $\mathbb{R}^2$ et soient $P \in (BC)$, $Q \in (CA)$, $R \in (AB)$ des points tous différents de $A, B, C$. On suppose que les droites $(PQ)$ et $(AB)$ ne sont pas parallèles.

**a)** Montrer qu'il existe une homothétie $h$ de centre $Q$ telle que $h(C) = A$ et une homothétie $h'$ de centre $P$ telle que $h'(B) = C$.

**b)** Calculer $h \circ h'(B)$. Montrer que le vecteur $\overrightarrow{PQ}$ n'est pas colinéaire à $\overrightarrow{AB}$. En déduire que $h \circ h'$ est une homothétie dont le centre appartient à $(AB)$ et $(PQ)$.

**c)** Montrer que les points $P, Q, R$ sont alignés si et seulement si $R$ est le centre de l'homothétie $h \circ h'$.

**d)** Montrer que les points $P, Q, R$ sont alignés si et seulement si $\frac{\overline{PC}}{\overline{PB}}\frac{\overline{QA}}{\overline{QC}}\frac{\overline{RB}}{\overline{RA}} = 1$.

**11.** Pour tout point $P \in \mathbb{R}^2$, notons $s_P : \mathbb{R}^2 \to \mathbb{R}^2$ la symétrie par rapport à $P$.

**a)** Soient $P$ et $Q$ des points de $\mathbb{R}^2$. Montrer que $s_Q \circ s_P$ est la translation de vecteur $2\overrightarrow{PQ}$.

**b)** Soient $I, J, K, L$ des points de $\mathbb{R}^2$. Montrer que $s_L \circ s_K \circ s_J \circ s_I$ est une translation. Quel est le vecteur de cette translation ?

**c)** Soient $I, J, K, L$ des points de $\mathbb{R}^2$. Montrer qu'il existe des points $A, B, C, D$ de $\mathbb{R}^2$ tels que $I$ est le milieu de $AB$, $J$ est le milieu de $BC$, $K$ est le milieu de $CD$ et $L$ est le milieu de $AD$ si et seulement si on a $\overrightarrow{IJ} = \overrightarrow{LK}$.

**12.** Soient $\mathcal{D}_1$ et $\mathcal{D}_2$ des droites parallèles de $\mathbb{R}^2$ et de direction $D$. Soit $D'$ une droite vectorielle supplémentaire de $D$. Notons $s_1$ la symétrie par rapport à $\mathcal{D}_1$ parallèlement à $D'$ et $s_2$ la symétrie par rapport à $\mathcal{D}_2$ parallèlement à $D'$.

**a)** Montrer qu'il existe un vecteur $u \in \mathbb{R}^2$ tel que $s_2(s_1(M)) - M = u$ quel que soit $M \in \mathbb{R}^2$.

**b)** En déduire que $s_2 \circ s_1$ est une translation.



## Quelques réponses ou indications

2. Une équation de $(ABC)$ est $2x - 4y - z + 5 = 0$.

4. b) Le plan $\mathscr{P}$ est le plan $(ABC)$. Une équation de $\mathscr{P}$ est $3x + y - 2z - 3 = 0$.

5. c) On a $s(x, y, z) = (y - z + 2, y, -x + y + 2)$.

d) Une équation de $s(\mathscr{Q})$ est $x - 2y + z - 4 = 0$.

6. c) On a $h(A) = P$ par définition de $k$. Le point $h(B)$ appartient à $(OB)$, le vecteur $\overrightarrow{h(A)h(B)} = k\overrightarrow{AB}$ appartient à la direction de $\mathscr{P}$, donc $h(B) \in \mathscr{P}$.

d) On a $\overrightarrow{GA} = -2\overrightarrow{GI}$.

e) Si $k \neq -1/2$, alors $h \circ h'$ est une homothétie. Si $k = -1/2$, alors $h \circ h'$ est une translation.

7. b) Si $M$ a pour coordonnées $u, v$, alors $M_1$ a pour coordonnées $0, v$.

c) Une équation de $(BC)$ est $x + y - 1 = 0$.

8. b) Les coordonnées de $F$ sont $\frac{q(r-1)}{r-q}$ et $\frac{r(q-1)}{q-r}$.

9. a) On a $\frac{\overline{PC}}{\overline{PB}} = \frac{u}{1-u}$.

c) Trouver des équations des droites $(AP)$, $(BQ)$ et $(CR)$.

10. b) Raisonner par l'absurde en supposant que $h \circ h'$ est une translation de vecteur $u$. Alors le vecteur $u$ n'est pas nul, car $h \circ h' \neq \mathrm{id}_{\mathbb{R}^2}$. De plus, $u$ est colinéaire à $\overrightarrow{PQ}$ et à $\overrightarrow{B(h \circ h'(B))} = \overrightarrow{BA}$, ce qui est impossible puisque les droites $(PQ)$ et $(AB)$ ne sont pas parallèles.

d) Le rapport de $h$ est $\frac{\overline{QA}}{\overline{QC}}$, celui de $h'$ est $\frac{\overline{PC}}{\overline{PB}}$ et celui de $h \circ h'$ est le produit de ces deux nombres.

11. a) On a $s_P(M) = 2P - M$ pour tous points $P$ et $M$ de $\mathbb{R}^2$.

b) Le vecteur de la translation est $2\overrightarrow{IJ} + 2\overrightarrow{KL}$.

c) Si $t_u$ est la translation de vecteur $u$, alors $u = 0$ si et seulement s'il existe un point $M$ tel que $t_u(M) = M$.

12. a) Choisir un point $A_1 \in \mathcal{D}_1$ et un point $A_2 \in \mathcal{D}_2$.

# Chapitre 9

# Arithmétique

On rappelle que l'on note $\mathbb{Z}$ l'ensemble des entiers relatifs, $\mathbb{N}$ l'ensemble des entiers naturels et qu'un entier naturel différent de 0 s'appelle un entier positif. Dans ce chapitre, un entier relatif sera appelé plus simplement un entier.

## 1. Divisibilité

**Définition**

Soient $a$ et $b$ des entiers. On dit que $a$ *divise* $b$, ou que $a$ est un *diviseur* de $b$, ou encore que $b$ est un *multiple* de $a$ s'il existe un entier $q$ tel que $b = aq$.

**Exemples**

- Tout entier divise 0. Le seul multiple de 0 est 0.
- Tout entier est multiple de 1 et de $-1$.
- Si $n$ est un entier non nul, alors $n$ et $-n$ sont des multiples et des diviseurs de $n$.
- L'entier $908\,070\,605\,040\,302\,010$ est multiple de 9.
- Si $n$ et $p$ sont des entiers positifs tels que $p \leqslant n$, alors $p!(n-p)!$ divise $n!$.

**Lemme.** *Soit $b$ un entier non nul. Si $a$ est un diviseur de $b$, alors il existe un unique entier $q$ tel que $b = aq$.*

**Démonstration.** Soient $q_1$ et $q_2$ des entiers tels que $b = aq_1$ et $b = aq_2$. Il vient $aq_1 - aq_2 = 0$, donc $a(q_1 - q_2) = 0$. Puisque $b$ est non nul, $a$ est non nul. Or un produit d'entiers non nuls est non nul, par suite on a $q_1 - q_2 = 0$, c'est-à-dire $q_1 = q_2$. ■

**Lemme.** *Soit $n$ un entier positif. Si $d$ est un diviseur de $n$, alors on a $-n \leqslant d \leqslant n$.*

**Démonstration.** Soit $d$ un diviseur de $n$. Il existe donc un entier $q$ tel que $dq = n$. Si $d$ est positif, alors $q$ aussi ; il s'ensuit que l'entier $n - d = d(q-1)$ est positif ou nul, par suite $0 \leqslant d \leqslant n$. Si $d$ est négatif, alors $-d$ est un diviseur positif de $n$, donc on a $0 \leqslant -d \leqslant n$, ou encore $-n \leqslant d \leqslant 0$. ∎

On en déduit qu'un entier non nul n'a qu'un nombre fini de diviseurs. En particulier, les seuls diviseurs de 1 sont 1 et $-1$.

**Lemme.** *Soient $a, b, c$ des entiers.*

- *Si $a$ divise $b$ et si $b$ divise $c$, alors $a$ divise $c$.*
- *Si $a$ divise $b$ et si $b$ divise $a$, alors $b = \pm a$.*
- *Si $a$ divise $b$ et $c$, alors $a$ divise $b + c$.*

**Démonstration.** Si $a$ divise $b$ et si $b$ divise $c$, il existe des entiers $q_1$ et $q_2$ tels que $aq_1 = b$ et $bq_2 = c$. Il vient $(aq_1)q_2 = c$, ou encore $a(q_1q_2) = c$, par suite $a$ divise $c$.

Si $a$ divise $b$ et si $b$ divise $a$, il existe des entiers $q_1$ et $q_2$ tels que $aq_1 = b$ et $bq_2 = a$. Si $a = 0$, alors $b$ est multiple de 0, donc $b = 0$ et l'on a bien le résultat. Supposons $a \neq 0$. Il vient $aq_1q_2 = a$, ou encore $a(1 - q_1q_2) = 0$. Il s'ensuit $1 - q_1q_2 = 0$, c'est-à-dire $q_1q_2 = 1$. En particulier $q_1$ est un diviseur de 1, donc $q_1 = 1$ ou $q_1 = -1$. On a ainsi démontré que $b = a$ ou $b = -a$.

Si $a$ divise $b$ et $c$, il existe des entiers $q_1$ et $q_2$ tels que $aq_1 = b$ et $aq_2 = c$. Il vient $b + c = aq_1 + aq_2 = a(q_1 + q_2)$. L'entier $b + c$ est donc multiple de $a$. ∎

**Proposition.** *Soit $b$ un entier positif. Si $a$ est un entier, alors il existe des entiers $q$ et $r$ uniques tels que $a = bq + r$ et $0 \leqslant r < b$.*

**Démonstration.** Démontrons l'existence de ces entiers. Si $a = 0$, il suffit de prendre $q = 0$ et $r = 0$. Si $a \neq 0$, traitons le cas $a > 0$ et déduisons le cas $a < 0$.

Supposons $a > 0$. Alors il existe un entier naturel $n$ tel que $bn \leqslant a$, par exemple $n = 0$. D'autre part, si $n$ est un entier naturel, on a $n \leqslant bn$, puisque $b$ est positif. Il s'ensuit que tout entier naturel $n$ tel que $bn \leqslant a$ est plus petit ou égal à $a$. Il n'y a ainsi qu'un nombre fini d'entiers naturels $n$ tels que $bn \leqslant a$. Notons $q$ le plus grand d'entre eux. Il vient $bq \leqslant a < b(q+1)$, c'est-à-dire $bq \leqslant a < bq + b$. Posons alors $r = a - bq$. On a $a = bq + r$ et $0 \leqslant r < b$.

Supposons $a < 0$. D'après ce qui précède, il existe des entiers $q'$ et $r'$ tels que $-a = bq' + r'$ et $0 \leqslant r' < b$. Si $r' = 0$, les entiers $q = -q'$ et $r = 0$ conviennent et si $r' \neq 0$, il suffit de prendre $q = -(q' + 1)$ et $r = b - r'$.

Démontrons l'unicité de ces entiers. Soient $q_1$ et $r_1$ des entiers vérifiant les conditions de la proposition, ainsi que $q_2$ et $r_2$. On a $bq_1 + r_1 = bq_2 + r_2$, soit $b(q_1 - q_2) = r_2 - r_1$. D'autre part on a $0 \leqslant r_1 < b$, donc $-b < -r_1 \leqslant 0$. Mais on a aussi $0 \leqslant r_2 < b$. En ajoutant ces inégalités, il vient $-b < r_2 - r_1 < b$, c'est-à-dire $-b < b(q_1 - q_2) < b$. Or



l'entier $b$ est positif, donc on a $-1 < q_1 - q_2 < 1$. Il s'ensuit $q_1 - q_2 = 0$, ou encore $q_1 = q_2$. Puisque $r_2 - r_1 = b(q_1 - q_2)$, on en déduit $r_1 = r_2$. ∎

**Définitions**

Dans la proposition ci-dessus, l'entier $q$ s'appelle le *quotient* et l'entier $r$ le *reste de la division euclidienne* de $a$ par $b$.

Soient $a$ un entier et $b$ un entier positif. D'après l'unicité énoncée dans la proposition ci-dessus, $b$ divise $a$ si et seulement si le reste de la division euclidienne de $a$ par $b$ est nul. Dans ce cas, le quotient de la division euclidienne de $a$ par $b$ s'appelle plus simplement le quotient de $a$ par $b$.

**Exemples**

- On a $45 = 19 \times 2 + 7$ donc 2 est le quotient et 7 le reste de la division euclidienne de 45 par 19.
- On a $-45 = -19 \times 3 + 12$ donc $-3$ est le quotient et 12 le reste de la division euclidienne de $-45$ par 19.

**Application.** Soit $x$ un nombre rationnel. Alors il existe un unique entier $q$ tel que $q \leqslant x < q + 1$. Écrivons en effet $x = a/b$, où $a$ est un entier et $b$ un entier positif. Si $q$ est le quotient de la division euclidienne de $a$ par $b$, alors le reste est $a - bq$, donc on a $0 \leqslant a - bq < b$. Puisque $b > 0$, l'entier $q$ vérifie les égalités demandées, ce qui démontre l'existence. D'autre part, si $q_1$ et $q_2$ sont des entiers tels que $q_1 \leqslant x < q_1 + 1$ et $q_2 \leqslant x < q_2 + 1$, il vient $q_1 < q_2 + 1$ et $q_2 < q_1 + 1$, d'où $-1 < q_1 - q_2 < 1$ et par suite $q_1 = q_2$, ce qui démontre l'unicité.

## 2. Plus grand commun diviseur

Si $a$ et $b$ sont des entiers, 1 est un diviseur de $a$ et $b$. D'autre part, un entier non nul n'a qu'un nombre fini de diviseurs. Ces deux propriétés permettent d'introduire la définition suivante.

**Définition**

Soient $a$ et $b$ des entiers non tous deux nuls. Le plus grand entier qui divise $a$ et $b$ s'appelle le *plus grand commun diviseur* de $a$ et $b$ et se note $\mathrm{pgcd}(a, b)$.

**Exemples**

- Si $a$ est un entier positif, on a $\mathrm{pgcd}(a, 0) = a$.
- Pour tout $a \in \mathbb{N}$, on a $\mathrm{pgcd}(a, 1) = 1$.

- Si $a$ est un entier et si $b$ est un diviseur positif de $a$, alors $\text{pgcd}(a,b) = b$.
- On a $\text{pgcd}(8,12) = 4$.

**Proposition.** *Soient $a$ et $b$ des entiers positifs. Si $r$ est le reste de la division euclidienne de $a$ par $b$, alors $\text{pgcd}(a,b) = \text{pgcd}(b,r)$.*

**Démonstration.** Notons $q$ le quotient de la division euclidienne de $a$ par $b$. Il vient $a = bq + r$. Si $d$ est un diviseur de $a$ et $b$, alors $d$ divise $a$ et $bq$, donc $a - bq$, c'est-à-dire $d$ divise $r$. Réciproquement, si $\delta$ est un diviseur de $b$ et $r$, alors $\delta$ divise $r$ et $bq$ donc $bq + r$, c'est-à-dire $\delta$ divise $a$. On a ainsi démontré que les diviseurs de $a$ et $b$ sont exactement les diviseurs de $b$ et $r$. En particulier, on a $\text{pgcd}(a,b) = \text{pgcd}(b,r)$. ∎

La proposition ci-dessus permet de présenter un algorithme de calcul du plus grand commun diviseur.

### L'algorithme d'Euclide

Soient $a$ et $b$ des entiers positifs tels que $a \geqslant b$. Notons $r_1$ le reste de la division euclidienne de $a$ par $b$. On vient de démontrer que l'on a $\text{pgcd}(a,b) = \text{pgcd}(b,r_1)$.

Si $r_1$ est nul, alors $\text{pgcd}(a,b) = \text{pgcd}(b,0) = b$.

Si $r_1$ n'est pas nul, posons $r_0 = b$ et notons $r_2$ le reste de la division euclidienne de $r_0$ par $r_1$. D'après la proposition précédente, on a $\text{pgcd}(r_0,r_1) = \text{pgcd}(r_1,r_2)$.

Si $r_2$ est nul, alors on a $\text{pgcd}(a,b) = \text{pgcd}(r_0,r_1) = \text{pgcd}(r_1,0) = r_1$.

Si $r_2$ n'est pas nul, définissons de proche en proche les entiers $r_n$ de la manière suivante : si $n \geqslant 3$ et si $r_{n-1} > 0$, alors $r_n$ est le reste de la division euclidienne de $r_{n-2}$ par $r_{n-1}$. Puisqu'on a

$$0 \leqslant r_n < r_{n-1} < \cdots < r_2 < r_1 < r_0,$$

il existe un entier $N \geqslant 2$ tel que $r_N > 0$ et tel que le reste de la division euclidienne de $r_{N-1}$ par $r_N$ est nul. D'après la proposition précédente, on a alors

$$\text{pgcd}(a,b) = \text{pgcd}(r_0,r_1) = \text{pgcd}(r_1,r_2) = \cdots = \text{pgcd}(r_{N-1},r_N) = \text{pgcd}(r_N,0) = r_N.$$

**Exemple.** Pratiquons l'algorithme d'Euclide pour calculer le plus grand commun diviseur de 585 et 247. Il vient successivement

$$585 = 247 \times 2 + 91$$
$$247 = 91 \times 2 + 65$$
$$91 = 65 \times 1 + 26$$
$$65 = 26 \times 2 + 13$$
$$26 = 13 \times 2 + 0$$



et le plus grand commun diviseur de 585 et 247 est ainsi égal à 13.

> Pour calculer le plus grand commun diviseur, disposez les divisions euclidiennes les unes sous les autres : le plus grand commun diviseur est le dernier reste non nul.

**Définition**

Soient $a$ et $b$ des entiers non tous deux nuls. On dit que $a$ et $b$ sont *premiers entre eux* si $\text{pgcd}(a,b) = 1$.

**Lemme.** *Si $a$ et $b$ sont des entiers non nuls, alors les quotients de $a$ et $b$ par $\text{pgcd}(a,b)$ sont des entiers premiers entre eux.*

**Démonstration.** Posons $d = \text{pgcd}(a,b)$ et $d' = \text{pgcd}(a',b')$, où $a'$ et $b'$ sont les quotients respectifs de $a$ et $b$ par $d$. On a $a = da'$ et $d'$ divise $a'$, donc $dd'$ divise $a$. De même, $dd'$ divise $b$. Ainsi $dd'$ est un diviseur commun de $a$ et $b$ donc $dd' \leqslant d$, ou encore $d(1-d') \geqslant 0$. Or on a $d > 0$, par suite $1 - d' \geqslant 0$. Puisque $d' > 0$, on en déduit $d' = 1$. ∎

## 3. Le théorème de Bézout

Si $a$ et $b$ sont des entiers positifs, alors pour tous entiers $x$ et $y$, $\text{pgcd}(a,b)$ divise $ax + by$. Il s'ensuit que si l'équation $ax + by = c$ a des solutions entières, alors $c$ est multiple de $\text{pgcd}(a,b)$. Nous allons démontrer que réciproquement, si $c$ est multiple de $\text{pgcd}(a,b)$, alors il existe $x, y \in \mathbb{Z}$ tels que $c = ax + by$. De plus, nous apprendrons à calculer explicitement tous ces entiers $x$ et $y$.

**Théorème de Bézout.** *Si $a$ et $b$ sont des entiers positifs, alors il existe des entiers $u$ et $v$ tels que $\text{pgcd}(a,b) = au + bv$.*

**Démonstration.** Supposons par exemple $a \geqslant b$ et notons $r_1$ le reste de la division euclidienne de $a$ par $b$. Si $r_1 = 0$, alors $\text{pgcd}(a,b) = b$ et l'on a $b = a \times 0 + b \times 1$.

Supposons $r_1 \neq 0$, posons $r_0 = b$, notons $q_1$ le quotient de la division euclidienne de $a$ par $b$ et $r_2$ le reste de la division euclidienne de $r_0$ par $r_1$. Il vient $a = bq_1 + r_1$ et l'on a $r_1 = a \times 1 + b \times (-q_1)$. Si $r_2 = 0$, alors on a $\text{pgcd}(a,b) = r_1$, donc $\text{pgcd}(a,b)$ est bien de la forme voulue.

Supposons désormais $r_2 \neq 0$ et démontrons par récurrence que pour chaque reste $r$ obtenu au cours de l'algorithme d'Euclide, il existe des entiers $x$ et $y$ tels que $r = ax + by$. Notons $r_N$ le dernier reste non nul et pour tout entier $n$ tel que $2 \leqslant n \leqslant N$, notons $q_n$ le quotient et $r_n$ le reste de la division euclidienne de $r_{n-2}$ par

$r_{n-1}$. On a $r_{n-2} = r_{n-1}q_n + r_n$, d'où $r_n = r_{n-2} - r_{n-1}q_n$. Supposons par récurrence qu'il existe des entiers $x, y, z, t$ tels que $r_{n-2} = ax + by$ et $r_{n-1} = az + bt$. Il vient

$$r_n = ax + by - (az + bt)q_n = a(x - q_n z) + b(y - q_n t),$$

donc $r_n$ est bien de la forme voulue. En particulier, le reste $r_N = \mathrm{pgcd}(a, b)$ est de la forme $au + bv$, où $u$ et $v$ sont des entiers. ■

Revenons à notre équation $ax + by = c$, où $a$ et $b$ sont des entiers positifs. Supposons que $c$ est multiple de $\mathrm{pgcd}(a, b)$, c'est-à-dire $c = k\,\mathrm{pgcd}(a, b)$ où $k \in \mathbb{Z}$. D'après le théorème de Bézout, il existe des entiers $u$ et $v$ tels que $au + bv = \mathrm{pgcd}(a, b)$. En multipliant par $k$, on en déduit $a(ku) + b(kv) = c$, donc l'équation $ax + by = c$ a des solutions entières.

### Calcul pratique

Pour trouver une *relation de Bézout* entre $a$ et $b$, c'est-à-dire pour trouver des entiers $u$ et $v$ tels que $\mathrm{pgcd}(a, b) = au + bv$, il faut tout d'abord pratiquer l'algorithme d'Euclide. Voici comment utiliser le calcul matriciel pour trouver ensuite une relation de Bézout. Pour décrire cette méthode, reprenons l'exemple donné dans le paragraphe précédent. Le plus grand commun diviseur de 585 et 247 est égal à 13 et les divisions euclidiennes successives sont les suivantes :

$$585 = 247 \times 2 + 91$$
$$247 = 91 \times 2 + 65$$
$$91 = 65 \times 1 + 26$$
$$65 = 26 \times 2 + 13.$$

On a donc $91 = 585 - 247 \times 2$, égalité que l'on traduit matriciellement par

$$\begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 585 \\ 247 \end{bmatrix} = \begin{bmatrix} 91 \\ 247 \end{bmatrix}.$$

De même, on a $65 = 247 - 91 \times 2$ et l'égalité matricielle

$$\begin{bmatrix} 1 & 0 \\ -2 & 1 \end{bmatrix} \begin{bmatrix} 91 \\ 247 \end{bmatrix} = \begin{bmatrix} 91 \\ 65 \end{bmatrix}.$$

On en déduit

$$\begin{bmatrix} 1 & 0 \\ -2 & 1 \end{bmatrix} \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 585 \\ 247 \end{bmatrix} = \begin{bmatrix} 91 \\ 65 \end{bmatrix}.$$

En effectuant le produit des deux matrices écrites à gauche (voir au chapitre 4, paragraphe 2 comment on multiplie à gauche par une matrice élémentaire), il vient

$$\begin{bmatrix} 1 & -2 \\ -2 & 5 \end{bmatrix} \begin{bmatrix} 585 \\ 247 \end{bmatrix} = \begin{bmatrix} 91 \\ 65 \end{bmatrix}.$$



Poursuivons en écrivant la troisième division euclidienne sous la forme

$$\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 91 \\ 65 \end{bmatrix} = \begin{bmatrix} 26 \\ 65 \end{bmatrix}.$$

On obtient

$$\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -2 \\ -2 & 5 \end{bmatrix} \begin{bmatrix} 585 \\ 247 \end{bmatrix} = \begin{bmatrix} 26 \\ 65 \end{bmatrix} \quad \text{et} \quad \begin{bmatrix} 3 & -7 \\ -2 & 5 \end{bmatrix} \begin{bmatrix} 585 \\ 247 \end{bmatrix} = \begin{bmatrix} 26 \\ 65 \end{bmatrix}.$$

Enfin, on a

$$\begin{bmatrix} 1 & 0 \\ -2 & 1 \end{bmatrix} \begin{bmatrix} 26 \\ 65 \end{bmatrix} = \begin{bmatrix} 26 \\ 13 \end{bmatrix}$$

d'où les égalités

$$\begin{bmatrix} 1 & 0 \\ -2 & 1 \end{bmatrix} \begin{bmatrix} 3 & -7 \\ -2 & 5 \end{bmatrix} \begin{bmatrix} 585 \\ 247 \end{bmatrix} = \begin{bmatrix} 26 \\ 13 \end{bmatrix} \quad \text{et} \quad \begin{bmatrix} 3 & -7 \\ -8 & 19 \end{bmatrix} \begin{bmatrix} 585 \\ 247 \end{bmatrix} = \begin{bmatrix} 26 \\ 13 \end{bmatrix}.$$

En particulier, on en déduit la relation de Bézout $-8 \times 585 + 19 \times 247 = 13$.

Le théorème de Bézout est très important. Les résultats qui suivent s'en déduisent et sont très utilisés.

**Théorème.** *Si $a$ et $b$ sont des entiers positifs, alors $a$ et $b$ sont premiers entre eux si et seulement s'il existe des entiers $u$ et $v$ tels que $au + bv = 1$.*

**Démonstration.** Si $a$ et $b$ sont premiers entre eux, le théorème de Bézout affirme l'existence de $u$ et $v$. Réciproquement, s'il existe des entiers $u$ et $v$ tels que $au + bv = 1$ et si $\delta$ est un diviseur de $a$ et $b$, alors $\delta$ divise $au$ et $bv$ donc $\delta$ divise $au + bv$, par suite $\delta = \pm 1$. En particulier, on a $\mathrm{pgcd}(a, b) = 1$. ■

**Proposition.** *Soient $a$ et $b$ des entiers positifs.*

- *Tout diviseur de $a$ et $b$ divise $\mathrm{pgcd}(a, b)$.*
- *Pour tout entier positif $n$, on a $\mathrm{pgcd}(na, nb) = n\,\mathrm{pgcd}(a, b)$.*

**Démonstration.** Posons $d = \mathrm{pgcd}(a, b)$.

Soit $\delta$ un diviseur de $a$ et $b$. Puisque $\delta$ divise $a$ et $b$, $\delta$ divise $au$ et $bv$ pour tous $u, v \in \mathbb{Z}$ donc $\delta$ divise $au + bv$ pour tous $u, v \in \mathbb{Z}$. En particulier, on en déduit d'après le théorème de Bézout que $\delta$ divise $d$.

Puisque $d$ divise $a$ et $b$, $nd$ divise $na$ et $nb$. D'après ce qui précède, $nd$ divise $\mathrm{pgcd}(na, nb)$. Mais $n$ divise $nd$, par suite $n$ divise $\mathrm{pgcd}(na, nb)$. Notons $k$ l'entier positif tel que $\mathrm{pgcd}(na, nb) = nk$. Puisque $nk$ divise $na$ et $nb$ et puisque $n$ n'est pas nul, $k$ divise $a$ et $b$. D'après ce qui précède, on en déduit que $k$ divise $d$. Il s'ensuit que $\mathrm{pgcd}(na, nb)$ divise $nd$. On a ainsi démontré que $nd$ divise $\mathrm{pgcd}(na, nb)$ et que $\mathrm{pgcd}(na, nb)$ divise $nd$, donc $\mathrm{pgcd}(na, nb) = \pm nd$. Or $nd > 0$ et $\mathrm{pgcd}(na, nb) > 0$, par suite $\mathrm{pgcd}(na, nb) = nd$. ■

**Théorème de Gauss.** *Soient $a$, $b$ et $c$ des entiers positifs. Si $a$ divise $bc$ et si $a$ et $b$ sont premiers entre eux, alors $a$ divise $c$.*

**Démonstration.** D'après la proposition précédente, on a $\text{pgcd}(ac, bc) = c\,\text{pgcd}(a, b)$. Or $a$ et $b$ sont premiers entre eux, par suite on a $\text{pgcd}(a, b) = 1$, d'où $\text{pgcd}(ac, bc) = c$. Puisque $a$ divise $ac$ et $a$ divise $bc$ par hypothèse, on en déduit également d'après la proposition précédente que $a$ divise $\text{pgcd}(ac, bc)$, c'est-à-dire que $a$ divise $c$. ∎

**Application.** Si $x$ est un nombre rationnel positif, alors il existe un unique couple $(a, b)$ d'entiers positifs et premiers entre eux tel que $x = a/b$. En effet, soient $y$ et $z$ des entiers positifs tels que $x = y/z$. Prenons pour $a$ et $b$ les quotients respectifs de $y$ et $z$ par $\text{pgcd}(y, z)$. On a $x = a/b$ et d'après le lemme page 193, $a$ et $b$ sont premiers entre eux. De plus, si $c$ et $d$ sont des entiers positifs et premiers entre eux tels que $c/d = a/b$, on a $ad = bc$. Ainsi $a$ divise $bc$. Or $a$ et $b$ sont premiers entre eux donc $a$ divise $c$, d'après le théorème de Gauss. Par le même raisonnement, on en déduit que $c$ divise $a$. Il s'ensuit $c = \pm a$, donc $c = a$, puisque $a$ et $c$ sont positifs. Enfin, puisque $c = a$, $ad = bc$ et $a \neq 0$, on a $d = b$.

**Résolution de l'équation $ax + by = c$.** Si $a$ et $b$ sont des entiers positifs et si $c$ est un entier, nous savons que l'équation $ax + by = c$ possède des solutions entières si et seulement si $\text{pgcd}(a, b)$ divise $c$. Nous allons voir dans l'exercice suivant comment le théorème de Gauss permet de trouver toutes les solutions d'une telle équation, lorsqu'on en connaît une solution particulière.

**Exercice**

a) Existe-t-il des entiers $x$ et $y$ tels que $161x + 368y = 15$ ? Si oui, trouver tous les entiers $x$ et $y$ tels que $161x + 368y = 15$.

b) Existe-t-il des entiers $x$ et $y$ tels que $161x + 368y = 115$ ? Si oui, trouver tous les entiers $x$ et $y$ tels que $161x + 368y = 115$.

**Réponse.** Calculons le plus grand commun diviseur de 161 et 368. Pratiquons pour cela l'algorithme d'Euclide. Il vient

$$368 = 161 \times 2 + 46$$
$$161 = 46 \times 3 + 23$$
$$46 = 23 \times 2 + 0$$

et le plus grand commun diviseur de 161 et 368 est ainsi égal à 23. En particulier, 23 est un diviseur de 161 et 368 ; précisément, on a $161 = 23 \times 7$ et $368 = 23 \times 16$. Il s'ensuit que pour tous $x, y \in \mathbb{Z}$, on a $161x + 368y = 23(7x + 16y)$, donc $161x + 368y$ est multiple de 23.

a) Puisque 15 n'est pas multiple de 23, il n'existe pas d'entiers $x$ et $y$ tels que $161x + 368y = 15$.





b) D'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que $161u + 368v = 23$. Puisque $115 = 23 \times 5$, il existe des entiers $x$ et $y$ tels que $161x + 368y = 115$, par exemple $x = 5u$ et $y = 5v$.

***Recherche d'une solution particulière.*** On a $46 = 368 - 161 \times 2$, qui se traduit matriciellement par

$$\begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 368 \\ 161 \end{bmatrix} = \begin{bmatrix} 46 \\ 161 \end{bmatrix}$$

et $23 = 161 - 46 \times 3$, qui se traduit matriciellement par

$$\begin{bmatrix} 1 & 0 \\ -3 & 1 \end{bmatrix} \begin{bmatrix} 46 \\ 161 \end{bmatrix} = \begin{bmatrix} 46 \\ 23 \end{bmatrix}.$$

Il vient alors

$$\begin{bmatrix} 46 \\ 23 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -3 & 1 \end{bmatrix} \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 368 \\ 161 \end{bmatrix} = \begin{bmatrix} 1 & -2 \\ -3 & 7 \end{bmatrix} \begin{bmatrix} 368 \\ 161 \end{bmatrix}.$$

En particulier, on en déduit la relation de Bézout $161 \times 7 - 368 \times 3 = 23$. En multipliant cette égalité par 5, il vient $161 \times 35 - 368 \times 15 = 115$.

***Recherche de toutes les solutions.*** Soient $x$ et $y$ des entiers tels que $161x + 368y = 115$. D'après ce qui précède, on a $161x + 368y = 161 \times 35 - 368 \times 15$, égalité que l'on écrit $368(y + 15) = 161(35 - x)$, ou encore $23 \times 16(y + 15) = 23 \times 7(35 - x)$. Il s'ensuit que l'on a $16(y + 15) = 7(35 - x)$.

En particulier, 16 divise $7(35 - x)$. Les entiers 7 et 16 sont premiers entre eux donc 16 divise $35 - x$, d'après le théorème de Gauss. Il existe ainsi $k \in \mathbb{Z}$ tel que $x - 35 = 16k$ et si l'on reporte cette égalité dans $16(y + 15) = 7(35 - x)$, il vient $y + 15 = -7k$. Finalement, on a $x = 35 + 16k$ et $y = -15 - 7k$. Réciproquement, on a $161(35 + 16k) - 368(15 + 7k) = 115$ pour tout $k \in \mathbb{Z}$.

Les entiers $x$ et $y$ tels que $161x + 368y = 115$ sont donc exactement les entiers de la forme $x = 35 + 16k$ et $y = -15 - 7k$, où $k \in \mathbb{Z}$.

Dans l'exercice précédent, on a ainsi trouvé explicitement toutes les solutions entières de l'équation $161x + 368y = 115$.

Voici un autre exercice utilisant le théorème de Gauss.

**Exercice.** Soient $a$, $b$ et $n$ des entiers positifs. Montrer que $n$ et $ab$ sont premiers entre eux si et seulement si $n$ et $a$ sont premiers entre eux ainsi que $n$ et $b$.

**Réponse.** Supposons que $n$ et $ab$ sont premiers entre eux. Tout entier qui divise $n$ et $a$ divise $n$ et $ab$, donc divise le pgcd de $n$ et $ab$. Puisque $\text{pgcd}(n, ab) = 1$, on en déduit que $n$ et $a$ sont premiers entre eux. De même, les entiers $n$ et $b$ sont premiers entre eux. Supposons que $n$ et $a$ sont premiers entre eux ainsi que $n$ et $b$. Soit $d$ un entier positif qui divise $n$ et $ab$. Tout diviseur positif commun à $d$ et $a$ divise $n$ et $a$, donc est égal à 1 puisque $n$ et $a$ sont premiers entre eux. Ainsi $d$ et $a$ sont premiers entre eux. Puisque $d$ divise $ab$, le théorème de Gauss affirme que $d$ divise $b$. Donc $d$ divise $n$ et $b$ et par suite $d = 1$. Cela montre que $n$ et $ab$ sont premiers entre eux.

## Plus petit commun multiple

**Proposition.** *Soient $a$ et $b$ des entiers positifs. Notons $m$ le quotient de $ab$ par $\text{pgcd}(a,b)$. L'entier $m$ est multiple de $a$ et $b$ et $m$ divise tout multiple de $a$ et $b$.*

**Démonstration.** Posons $d = \text{pgcd}(a,b)$ et notons $a'$ et $b'$ les entiers positifs tels que $a = da'$ et $b = db'$. Par définition de l'entier $m$, on a $md = ab$, donc $m = a'b = ab'$. Ainsi $m$ est multiple de $a$ et $b$. Soit $n$ un multiple de $a$ et $b$. Notons respectivement $k$ et $\ell$ les quotients de $n$ par $a$ et $b$. Il vient $ka = n = \ell b$, donc $ka'd = \ell b'd$, soit $d(ka' - \ell b') = 0$. Puisque $d \neq 0$, il s'ensuit $ka' = \ell b'$. En particulier, $a'$ divise $\ell b'$. Mais d'après le lemme page 193, $a'$ et $b'$ sont premiers entre eux donc $a'$ divise $\ell$, d'après le théorème de Gauss. Par suite $a'b$ divise $\ell b$, c'est-à-dire $m$ divise $n$. ∎

> **Définition**
> Soient $a$ et $b$ des entiers positifs. L'entier $m$ défini dans la proposition ci-dessus s'appelle le *plus petit commun multiple* de $a$ et $b$ et se note $\text{ppcm}(a,b)$.

Si les entiers $a$ et $b$ sont premiers entre eux, alors on a $\text{pgcd}(a,b) = 1$ et donc, par définition du plus petit commun multiple, il vient $\text{ppcm}(a,b) = ab$.

# 4. Les nombres premiers

> **Définition**
> Un *nombre premier* est un entier $p$ supérieur ou égal à 2 dont les seuls diviseurs positifs sont 1 et $p$.

### Exemples

- Les cinq premiers nombres premiers sont 2, 3, 5, 7 et 11.
- L'entier 9123 n'est pas premier : il est divisible par 3.
- L'entier $2^{13} - 1$ est premier (ce résultat fait l'objet d'un exercice en fin de chapitre).

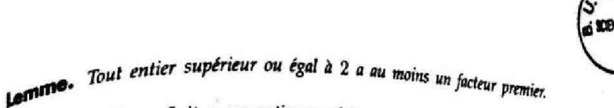
**Lemme.** *Soient $n$ un entier positif et $p$ un nombre premier. Alors ou bien $p$ divise $n$, ou bien $n$ et $p$ sont premiers entre eux.*

**Démonstration.** Notons $d$ le plus grand commun diviseur de $p$ et $n$. En particulier $d$ est un diviseur positif de $p$, par suite $d = 1$ ou $d = p$, d'où le résultat. ∎

> **Définition**
> Soit $n$ un entier supérieur ou égal à 2. Un nombre premier qui divise $n$ s'appelle un *facteur premier* de $n$.







**Lemme.** *Tout entier supérieur ou égal à 2 a au moins un facteur premier.*

**Démonstration.** Soit $n$ un entier supérieur ou égal à 2. Il existe un diviseur $k$ de $n$ tel que $k \geqslant 2$, par exemple $k = n$. Soit $p$ le plus petit diviseur de $n$ tel que $p \geqslant 2$. Si $k$ est un diviseur de $p$ et si $k \geqslant 2$, alors $k$ divise $n$ et par définition de $p$, on a $k \geqslant p$. Tout diviseur de $p$ supérieur ou égal à 2 est donc égal à $p$. Il s'ensuit que $p$ est un nombre premier. Or $p$ divise $n$, par suite $p$ est un facteur premier de $n$. ∎

**Proposition.** *Il existe une infinité de nombres premiers.*

**Démonstration.** Il existe au moins deux nombres premiers, par exemple 2 et 3. Raisonnons par l'absurde et supposons qu'il n'y a qu'un nombre fini de nombres premiers, notés $p_1, p_2, \ldots, p_n$. Considérons l'entier $N = 1 + p_1 p_2 \cdots p_n$, où $p_1 p_2 \cdots p_n$ est le produit des $p_i$. Puisque $N \geqslant 2$, il existe un facteur premier $p$ de $N$. Ce nombre premier $p$ est égal à l'un des $p_i$, par suite $p$ divise le produit $p_1 p_2 \cdots p_n$, donc $p$ divise $1 = N - p_1 p_2 \cdots p_n$. Mais cela est impossible, car les seuls diviseurs de 1 sont 1 et $-1$ et l'on a $p \geqslant 2$. ∎

**Proposition.** *Soit $n$ un entier supérieur ou égal à 2. Si $n$ n'est pas premier, alors il existe un facteur premier $p$ de $n$ tel que $p \leqslant \sqrt{n}$.*

**Démonstration.** Puisque $n$ n'est pas premier, il existe un diviseur $k$ de $n$ tel que $1 < k < n$. Soit $q$ le quotient de $n$ par $k$. Puisque $n = kq$, l'un des deux entiers $k$ ou $q$ est plus petit ou égal à $\sqrt{n}$. D'autre part, on a $1 < k < n$, donc on a aussi $1 < q < n$. Il suffit alors de prendre pour $p$ un facteur premier de celui des entiers $k$ ou $q$ qui est plus petit ou égal à $\sqrt{n}$. ∎

**Application.** Si $n$ est un entier tel que $n < 49$, il est très facile de savoir si $n$ est premier ou pas, puisque seules les divisions par 2, 3 ou 5 sont à tester. Si $n$ est un entier tel que $48 < n < 121$, alors $n$ est premier si et seulement si $n$ n'est pas divisible par 2, 3, 5 ou 7, ce qui n'est pas très difficile à tester non plus.
On en déduit ainsi la liste des nombres premiers plus petits que 121 : ce sont les entiers 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113.

**Lemme d'Euclide.** *Soient $a$ et $b$ des entiers positifs et $p$ un nombre premier. Si $p$ divise $ab$, alors $p$ divise $a$ ou $p$ divise $b$.*

**Démonstration.** Supposons que $p$ ne divise pas $a$. D'après le premier lemme de ce paragraphe, $p$ et $a$ sont premiers entre eux. Il s'ensuit que $p$ divise $b$ d'après le théorème de Gauss. ∎

**Application.** Soit $n$ un entier supérieur ou égal à 2. Les facteurs premiers de $n!$ sont les nombres premiers $p$ tels que $p \leqslant n$. En effet, puisque $n! = 2 \times \cdots \times n$, tout entier positif $k$ tel que $k \leqslant n$ divise $n!$. En particulier, tout nombre premier $p$ tel que $p \leqslant n$ divise $n!$. Réciproquement, si $p$ est un facteur premier du produit $2 \times \cdots \times n$, alors d'après le lemme d'Euclide, $p$ divise l'un des termes du produit : il existe donc un entier $k$ vérifiant $2 \leqslant k \leqslant n$ tel que $p$ divise $k$. Il s'ensuit $p \leqslant n$.

**Proposition.** *Soit $p$ un nombre premier. Si $k$ est un entier tel que $0 < k < p$, alors $p$ divise le coefficient binomial $C_p^k$.*

**Démonstration.** Soit $k$ un entier tel que $0 < k < p$. Nous avons vu au chapitre 2 paragraphe 4 que l'on a $p! = k!(p-k)!C_p^k$. Puisque $p$ divise $p!$, l'entier $p$ divise l'un des entiers $k!$, $(p-k)!$ ou $C_p^k$, d'après le lemme d'Euclide. D'autre part, on a $k < p$ et $p - k < p$ par suite $p$ ne divise ni $k!$, ni $(p-k)!$. On en déduit que $p$ divise $C_p^k$. ■

**Théorème.** *Soit $n$ un entier supérieur ou égal à 2. Alors il existe un unique entier positif $r$ et des nombres premiers $p_1, \ldots, p_r$ uniques tels que $p_1 \leqslant \cdots \leqslant p_r$ et $n = p_1 \cdots p_r$.*

**Démonstration.** Démontrons l'existence d'une telle factorisation par récurrence. Si $n = 2$, alors $n$ est un nombre premier. Si $n \geqslant 3$, on sait que $n$ a au moins un facteur premier. Notons $p_1$ le plus petit facteur premier de $n$. Si $n$ est un nombre premier, alors $n = p_1$. Si $n$ n'est pas un nombre premier, notons $q$ le quotient de $n$ par $p_1$. Il vient $2 \leqslant q < n$. On applique alors l'hypothèse de récurrence à $q$.

Démontrons l'unicité également par récurrence. On suppose que $n$ se factorise sous la forme $n = p_1 \cdots p_r$, où les $p_i$ sont des nombres premiers tels que $p_1 \leqslant \cdots \leqslant p_r$ et se factorise aussi sous la forme $n = q_1 \cdots q_s$, où les $q_j$ sont des nombres premiers tels que $q_1 \leqslant \cdots \leqslant q_s$. Si $p_1 < q_1$, alors on a $1 < p_1 < q_j$ pour tout $j$ ; par suite $p_1$ ne divise aucun des nombres premiers $q_j$, donc ne divise pas le produit $q_1 \cdots q_s$, d'après le lemme d'Euclide. Or cela est impossible, d'où l'on a $p_1 \geqslant q_1$. De même on démontre que $q_1 \geqslant p_1$. Il s'ensuit $p_1 = q_1$. Si $n = p_1$, alors $s = 1$ et $q_1 = p_1$. Si $n > p_1$, on applique l'hypothèse de récurrence au quotient de $n$ par $p_1$. ■

Soit $a$ un entier positif. Pour tout nombre premier $p$, le plus grand entier naturel $n$ tel que $p^n$ divise $a$ s'appelle l'*exposant* de $p$ dans $a$. Par exemple, l'exposant de 2 dans $2^5 \times 7^4$ est 5 et l'exposant de 3 est 0.

**Application.** Soit $n$ un entier supérieur ou égal à 2 sans facteur carré. Autrement dit, il n'existe pas d'entier supérieur ou égal à 2 dont le carré divise $n$. Alors le nombre réel $\sqrt{n}$ est irrationnel, c'est-à-dire n'appartient pas à $\mathbb{Q}$. Pour le démontrer, raisonnons par l'absurde : supposons qu'il existe des entiers positifs $a$ et $b$ tels que $\sqrt{n} = a/b$. Élevons au carré : il vient $a^2 = nb^2$. Si $p$ est un facteur premier de $n$, alors





l'exposant de $p$ dans $nb^2$ est impair, puisque $p^2$ ne divise pas $n$. Or l'exposant de tout nombre premier dans $a^2$ est pair. Il y a donc contradiction, par suite $\sqrt{n}$ est irrationnel.

**Exercice**

a) L'entier $2^3 \times 5^3 \times 7^2$ divise-t-il $2^4 \times 3 \times 5^2 \times 7^5$ ?

b) Quels sont les diviseurs positifs de $2^4 \times 3 \times 5^2 \times 7^5$ ? Préciser le nombre de ces diviseurs.

c) Factoriser le plus grand commun diviseur de $2^3 \times 5^3 \times 7^2$ et $2^4 \times 3 \times 5^2 \times 7^5$ en produit de nombres premiers.

d) Factoriser le plus petit commun multiple de $2^3 \times 5^3 \times 7^2$ et $2^4 \times 3 \times 5^2 \times 7^5$ en produit de nombres premiers.

**Réponse**

a) Si $n$ est un multiple de $2^3 \times 5^3 \times 7^2$, alors $5^3$ divise $n$. D'autre part, 5 ne divise pas $2^4 \times 3 \times 7^5$ d'après le lemme d'Euclide, par suite $5^3$ ne divise pas $2^4 \times 3 \times 5^2 \times 7^5$. L'entier $2^4 \times 3 \times 5^2 \times 7^5$ n'est donc pas multiple de $2^3 \times 5^3 \times 7^2$.

b) Toujours en utilisant le lemme d'Euclide, on en déduit que l'exposant de 2 dans un diviseur de $2^4 \times 3 \times 5^2 \times 7^5$ est plus petit ou égal à 4. Le même raisonnement s'applique pour les autres facteurs premiers de $2^4 \times 3 \times 5^2 \times 7^5$. Par conséquent, les diviseurs positifs de $2^4 \times 3 \times 5^2 \times 7^5$ sont exactement les entiers qui s'écrivent $2^a \times 3^b \times 5^c \times 7^d$, où $a, b, c, d$ sont des entiers naturels tels que $a \leqslant 4$, $b \leqslant 1$, $c \leqslant 2$ et $d \leqslant 5$. Il y a ainsi cinq valeurs possibles pour $a$, deux pour $b$, trois pour $c$ et six pour $d$. L'entier $2^4 \times 3 \times 5^2 \times 7^5$ a donc $5 \times 2 \times 3 \times 6 = 180$ diviseurs positifs.

c) Pour les mêmes raisons que précédemment, l'exposant de 2 dans un diviseur commun à $2^3 \times 5^3 \times 7^2$ et $2^4 \times 3 \times 5^2 \times 7^5$ est plus petit ou égal à 3 et $2^3$ divise chacun de ces entiers. En raisonnant de même pour les autres facteurs premiers communs, on en déduit $\operatorname{pgcd}(2^3 \times 5^3 \times 7^2, 2^4 \times 3 \times 5^2 \times 7^5) = 2^3 \times 5^2 \times 7^2$.

d) Puisque $\operatorname{pgcd}(a,b)\operatorname{ppcm}(a,b) = ab$, il vient $\operatorname{ppcm}(2^3 \times 5^3 \times 7^2, 2^4 \times 3 \times 5^2 \times 7^5) = 2^4 \times 3 \times 5^3 \times 7^5$.

Si $a$ et $b$ sont des entiers positifs, alors pour tout nombre premier $p$,

- l'exposant de $p$ dans $\operatorname{pgcd}(a,b)$ est le plus petit des exposants de $p$ dans $a$ et $b$.
- l'exposant de $p$ dans $\operatorname{ppcm}(a,b)$ est le plus grand des exposants de $p$ dans $a$ et $b$.

Mais attention, on ne sait en général pas factoriser un entier grand en produit de nombres premiers. Pour calculer le plus grand commun diviseur de deux entiers positifs, la méthode sûre est la pratique de l'algorithme d'Euclide.

## 5. Congruences

Dans ce paragraphe, $n$ est un entier supérieur ou égal à 2.

**Définition**
Soient $a$ et $b$ des entiers. On dit que $a$ est *congru à $b$ modulo $n$* si $a-b$ est multiple de $n$. Cette propriété se note $a \equiv b\,[n]$.

**Exemples**
- Pour tout entier $a$, on a $a \equiv a\,[n]$.
- On a $2^7 \equiv 2\,[7]$.
- Pour tout $x \in \mathbb{Z}$, on a $7x^2 + 123x \equiv 15x^4 + x^2\,[3]$.

Regroupons dans un lemme les règles de calcul sur les congruences.

**Lemme.** *Soient $a, b, c, d$ des entiers.*
- *Si $a \equiv b\,[n]$, alors $b \equiv a\,[n]$.*
- *Si $a \equiv b\,[n]$ et $b \equiv c\,[n]$, alors $a \equiv c\,[n]$.*
- *Si $a \equiv b\,[n]$ et $c \equiv d\,[n]$, alors $a + c \equiv b + d\,[n]$ et $ac \equiv bd\,[n]$.*

**Démonstration.** Si $n$ divise $a-b$, alors $n$ divise $b-a$, d'où la première propriété.
Si $n$ divise $a-b$ et $b-c$, alors $n$ divise $(a-b)+(b-c) = a-c$, ce qui démontre la deuxième propriété.
Si $n$ divise $a-b$ et $c-d$, alors $n$ divise $(a-b)+(c-d) = (a+c)-(b+d)$ et $n$ divise $d(a-b)+a(c-d) = ac-bd$. La troisième propriété est ainsi démontrée. ∎

**Application** : divisibilité par 2, 3, 5, 9 ou 11.
- Puisque $10 \equiv 0\,[2]$, tout entier positif est congru modulo 2 à son chiffre des unités. Il s'ensuit qu'un entier positif est divisible par 2 si et seulement si son chiffre des unités est multiple de 2, c'est-à-dire est égal à 0, 2, 4, 6 ou 8.
- Puisque $10 \equiv 0\,[5]$, le même raisonnement s'applique en remplaçant 2 par 5. On en déduit qu'un entier positif est divisible par 5 si et seulement si son chiffre des unités est égal à 0 ou 5.
- Puisque $10 \equiv 1\,[9]$, tout entier positif est congru modulo 9 à la somme de ses chiffres. Il s'ensuit qu'un entier positif est divisible par 9 si et seulement si la somme de ses chiffres est multiple de 9. On a le même résultat en remplaçant 9 par 3.
- Puisque $10 \equiv -1\,[11]$, tout entier positif est congru modulo 11 à la somme alternée de ses chiffres $a_0 - a_1 + \cdots + (-1)^k a_k$, $a_0$ étant le chiffre des unités de $n$. Il s'ensuit qu'un entier positif est divisible par 11 si et seulement si la somme alternée de ses chiffres est multiple de 11.



**Proposition.** *Si $a$ est un entier, alors le reste de la division euclidienne de $a$ par $n$ est l'unique entier $x$ tel que $a \equiv x\,[n]$ et $0 \leqslant x < n$.*

**Démonstration.** Notons $q$ le quotient et $r$ le reste de la division euclidienne de $a$ par $n$. On a $0 \leqslant r < n$ et $a = nq + r$. L'entier $a - r$ est multiple de $n$, donc $a \equiv r\,[n]$. Supposons que $x$ est un entier tel que $a \equiv x\,[n]$ et $0 \leqslant x < n$. Puisque $a \equiv r\,[n]$, on a $x \equiv r\,[n]$ donc $x - r$ est multiple de $n$. Puisque $-n < x - r < n$, il s'ensuit $x - r = 0$, c'est-à-dire $x = r$. ∎

**Exemples**
- Si $a$ est un entier, alors ou bien $a \equiv 0\,[2]$ et l'on dit que $a$ est un entier *pair*, ou bien $a \equiv 1\,[2]$ et l'on dit que $a$ est un entier *impair*.
- Lorsqu'on divise un entier impair par 4, le reste est 1 ou 3. Si $a$ est un entier impair, on a donc $a \equiv 1\,[4]$ ou $a \equiv 3\,[4]$.

### Calcul d'une puissance modulo un entier

Si $a$ est un entier, *calculer $a$ modulo $n$* signifie calculer le reste de la division euclidienne de $a$ par $n$. De plus, si l'on a trouvé un entier $x$ tel que $a \equiv x\,[n]$ et $0 \leqslant x < n$, alors on sait que $x$ est le reste de la division euclidienne de $a$ par $n$.

Dégageons la méthode à utiliser à l'aide d'un exemple. Calculons $2^{18}$ modulo 37.

Ce qu'il ne faut pas faire, c'est calculer l'entier $2^{18}$ puis faire la division euclidienne de cet entier par 37.

Ce qu'il faut faire, c'est utiliser la compatibilité des congruences avec la multiplication. Pour cela, cherchons la puissance de 2 la plus proche de 37. On a $2^5 = 32$ et $2^6 = 64$ donc la puissance de 2 la plus proche de 37 est $2^5$. Puisque $32 = 37 - 5$, il vient $2^5 \equiv -5\,[37]$. En élevant au carré, on en déduit $(2^5)^2 \equiv (-5)^2\,[37]$, c'est-à-dire $2^{10} \equiv 25\,[37]$. Mais on a $25 = 37 - 12$, donc $2^{10} \equiv -12\,[37]$. En revenant à la définition d'une congruence, 37 divise ainsi $2^{10} + 12 = 2(2^9 + 6)$. Puisque 37 est un nombre premier, 37 divise $2^9 + 6$ d'après le lemme d'Euclide. Il s'ensuit $2^9 \equiv -6\,[37]$. En élevant de nouveau au carré, il vient $2^{18} \equiv 36\,[37]$, ou encore $2^{18} \equiv -1\,[37]$.

Nous venons de démontrer que 36 est le reste de la division euclidienne de $2^{18}$ par 37.

Voici des exercices où l'on utilise les congruences pour résoudre un problème d'arithmétique.

**Exercice 1.** Soient $x$ et $y$ des entiers. On suppose que $3x + 7y$ est multiple de 11. Montrer que $4x - 9y$ est multiple de 11.

> **Réponse.** Par hypothèse, on a $3x \equiv -7y\,[11]$. Puisque $5 \equiv 5\,[11]$, on en déduit $15x \equiv -35y\,[11]$. Or on a $15x = 4x + 11x$, donc $15x \equiv 4x\,[11]$ et $-35y = -44y + 9y$, donc $-35y \equiv 9y\,[11]$. Par suite il vient $4x \equiv 9y\,[11]$. L'entier $4x - 9y$ est donc multiple de 11.

**Exercice 2.** Si $a$ et $b$ sont des entiers, quel est le reste de la division de $a^2+b^2$ par 4 ? En déduire que si $p$ est un nombre premier différent de 2 et s'il existe des entiers $a$ et $b$ tels que $p=a^2+b^2$, alors $p-1$ est multiple de 4.

> **Réponse.** Le reste de la division euclidienne d'un entier par 4 est égal à 0, 1, 2 ou 3. Pour tout $x\in\mathbb{Z}$, $x^2$ est donc congru à 0, $1^2$, $2^2$ ou $3^2$ modulo 4. Or on a $2^2=4$, donc $2^2\equiv 0\,[4]$ et $3^2=9$, donc $3^2\equiv 1\,[4]$. Il s'ensuit que pour tout $x\in\mathbb{Z}$, $x^2$ est congru à 0 ou 1 modulo 4. Pour tous $a,b\in\mathbb{Z}$, $a^2+b^2$ est donc congru à 0, 1 ou 2 modulo 4. Un nombre premier différent de 2 est impair, par conséquent n'est pas congru à 0 ou 2 modulo 4. S'il s'écrit $p=a^2+b^2$, on a donc $p\equiv 1\,[4]$, d'où $p-1$ est multiple de 4.

**Exercice 3.** Montrer que pour tout entier $x$ non divisible par 3, $x^3$ est congru à 1 ou à $-1$ modulo 9. En déduire qu'il n'existe pas d'entiers $a,b,c$, tous non divisibles par 3 tels que $a^3+b^3=c^3$.

> **Réponse.** Soit $x$ un entier non divisible par 3. Puisque 3 est premier, les entiers $x$ et 3 sont premiers entre eux, donc $x$ et 9 aussi. Si $r$ est le reste de la division euclidienne de $x$ par 9, on a $\mathrm{pgcd}(x,9)=\mathrm{pgcd}(9,r)$, par suite $r$ et 9 sont premiers entre eux, donc $r$ est différent de 0, 3 et 6. Ainsi $x$ est congru à 1, 2, 4, 5, 7 ou 8 modulo 9 ou encore à $\pm1$, $\pm2$ ou $\pm4$ modulo 9, donc $x^3$ est congru à $\pm1$, $\pm2^3$ ou $\pm4^3$ modulo 9. Mais $2^3$ est congru à $-1$ modulo 9 et $4^3$ est congru à 1 modulo 9, par suite $x^3$ est congru à $\pm1$ modulo 9. Soient $a,b,c$ des entiers tous non divisibles par 3. D'après ce qui précède, $a^3+b^3$ est congru à 0, 2 ou $-2$ modulo 9 et $c^3$ à 1 ou $-1$. Il s'ensuit que $a^3+b^3$ n'est pas congru à $c^3$ modulo 9, donc $a^3+b^3$ est différent de $c^3$.

**Lemme.** *Si $a$ est un entier positif, alors il existe un entier $u$ tel que $au\equiv 1\,[n]$ si et seulement si $a$ et $n$ sont premiers entre eux.*

**Démonstration.** Soit $u\in\mathbb{Z}$. On a $au\equiv 1\,[n]$ si et seulement si $n$ divise $1-au$, c'est-à-dire si et seulement s'il existe $v\in\mathbb{Z}$ tel que $nv=1-au$, ou encore $au+nv=1$. Le résultat est ainsi démontré, grâce au théorème de Bézout. ∎

> Soient $a$ et $n$ des entiers positifs premiers entre eux. Pour trouver un entier $u$ tel que $au\equiv 1\,[n]$, cherchez une relation de Bézout entre $a$ et $n$.

## Résolution de l'équation $ax\equiv b\,[n]$

Soient $a$ un entier positif et $b$ un entier.

*Premier cas* : $a$ et $n$ sont premiers entre eux. D'après le lemme ci-dessus, il existe $u\in\mathbb{Z}$ tel que $au\equiv 1\,[n]$. Si $x$ est un entier tel que $ax\equiv b\,[n]$, en multipliant par $u$ on obtient $aux\equiv bu\,[n]$. Puisque $au\equiv 1\,[n]$, il vient $aux\equiv x\,[n]$, donc $x\equiv bu\,[n]$. Réciproquement, si $x\equiv bu\,[n]$, alors en multipliant par $a$ il vient $ax\equiv bau\,[n]$, d'où $ax\equiv b\,[n]$.

*Second cas* : $a$ et $n$ ne sont pas premiers entre eux. Posons $d=\mathrm{pgcd}(a,n)$. S'il existe un entier $x$ tel que $ax\equiv b\,[n]$, alors $n$ divise $b-ax$, par suite $d$ divise $b-ax$. Puisque $d$ divise $ax$, il s'ensuit que $d$ divise $(b-ax)+ax=b$. Si $d$ ne divise pas $b$, l'équation $ax\equiv b\,[n]$ n'a donc pas de solution.

Supposons que $d$ divise $b$. Notons $a'$, $b'$ et $n'$ les entiers tels que $a=da'$, $b=db'$ et $n=dn'$. Si $x$ est un entier, alors on a $ax\equiv b\,[n]$ si et seulement si $a'x\equiv b'\,[n']$. Puisque les entiers $a'$ et $n'$ sont premiers entre eux, il existe $u\in\mathbb{Z}$ tel que $ua'\equiv 1\,[n']$. On a alors $ua'x\equiv x\,[n']$ et $ua'x\equiv ub'\,[n']$, d'où $x\equiv ub'\,[n']$. Réciproquement, supposons que $x$ est un entier tel $x\equiv ub'\,[n']$. En multipliant par $a'$, il vient $a'x\equiv a'ub'\,[n]$, d'où $a'x\equiv b'\,[n]$. Les entiers $x$ tels que $ax\equiv b\,[n]$ sont les entiers $x$ tels que $x\equiv b'u\,[n']$.

**Exercice.** Soit $b\in\mathbb{Z}$. Existe-il $x\in\mathbb{Z}$ tel que $24x\equiv b\,[182]$ ? Si oui, trouver tous les entiers $x$ tels que $24x\equiv b\,[182]$.

> **Réponse.** Les factorisations en produit de nombres premiers de 24 et 182 sont $24=2^3\times 3$ et $182=2\times 7\times 13$. On a ainsi $\mathrm{pgcd}(24,182)=2$. On en déduit qu'il existe $x\in\mathbb{Z}$ tel que $24x\equiv b\,[182]$ si et seulement si $b$ est pair.
> Supposons $b$ pair et posons $b=2c$. Si $x$ est un entier, on a les équivalences
> $$24x\equiv 2c\,[182]\iff 182 \text{ divise } 24x-2c\iff 91 \text{ divise } 12x-c\iff 12x\equiv c\,[91].$$
> Cherchons une relation de Bézout entre 12 et 91 et pour cela, pratiquons l'algorithme d'Euclide. Il vient
> $$91=12\times 7+7$$
> $$12=7\times 1+5$$
> $$7=5\times 1+2$$
> $$5=2\times 2+1.$$
> On en déduit successivement
> $$\begin{bmatrix}1&-7\\0&1\end{bmatrix}\begin{bmatrix}91\\12\end{bmatrix}=\begin{bmatrix}7\\12\end{bmatrix},\quad \begin{bmatrix}1&-7\\-1&8\end{bmatrix}\begin{bmatrix}91\\12\end{bmatrix}=\begin{bmatrix}7\\5\end{bmatrix},$$
> $$\begin{bmatrix}2&-15\\-1&8\end{bmatrix}\begin{bmatrix}91\\12\end{bmatrix}=\begin{bmatrix}2\\5\end{bmatrix}\quad\text{et}\quad\begin{bmatrix}2&-15\\-5&38\end{bmatrix}\begin{bmatrix}91\\12\end{bmatrix}=\begin{bmatrix}2\\1\end{bmatrix}.$$
> En particulier, on a la relation de Bézout $12\times 38-91\times 5=1$. Lorsque $b$ est pair, les entiers $x$ tels que $24x\equiv b\,[182]$ sont donc les entiers $x$ tels que $x\equiv 38c\,[91]$.

Voici un théorème qui permet de résoudre simultanément deux congruences modulo des entiers premiers entre eux.

**Théorème chinois des restes.** *Soient $n$ et $k$ des entiers supérieurs ou égaux à 2 et premiers entre eux. Pour tous entiers $a$ et $b$, il existe un entier $x$ tel que* $\begin{cases}x\equiv a\,[n]\\x\equiv b\,[k]\end{cases}$.

**Démonstration.** Puisque les entiers $n$ et $k$ sont premiers entre eux, il existe $u, v \in \mathbb{Z}$ tels que $nu + kv = 1$. On a $kv - 1 = -nu$ donc $n$ divise $kv - 1$. De même $k$ divise $nu - 1$. Puisque $k$ divise $kv$ et $n$ divise $nu$, on en déduit

$$\begin{cases} kv \equiv 1\,[n] \\ kv \equiv 0\,[k] \end{cases} \quad \text{et} \quad \begin{cases} nu \equiv 0\,[n] \\ nu \equiv 1\,[k]. \end{cases}$$

Posons $x = akv + bnu$. Puisque $kv \equiv 1\,[n]$ et $nu \equiv 0\,[n]$, il vient $akv + bnu \equiv a\,[n]$, c'est-à-dire $x \equiv a\,[n]$. De même, on a $kv \equiv 0\,[k]$ et $nu \equiv 1\,[k]$, donc $akv + bnu \equiv b\,[k]$, c'est-à-dire $x \equiv b\,[k]$. ■

> Cette démonstration est extrêmement utile : c'est comme cela que vous trouverez un tel entier $x$ dans la pratique.

## Résolution du système d'équations $\begin{cases} x \equiv a\,[n] \\ x \equiv b\,[k] \end{cases}$

Soient $a$ et $b$ des entiers.

***Premier cas*** : $n$ et $k$ sont premiers entre eux. D'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que $nu + kv = 1$. Posons $x_0 = akv + bnu$. Nous venons de démontrer que l'on a $x_0 \equiv a\,[n]$ et $x_0 \equiv b\,[k]$.

Soit $x \in \mathbb{Z}$. On a $x \equiv a\,[n]$ et $x \equiv b\,[k]$ si et seulement si $x \equiv x_0\,[n]$ et $x \equiv x_0\,[k]$, c'est-à-dire si et seulement si $n$ et $k$ divisent $x - x_0$. On a donc $x \equiv a\,[n]$ et $x \equiv b\,[k]$ si et seulement si $x - x_0$ est multiple de $n$ et $k$.

D'autre part, un entier est multiple de $n$ et $k$ si et seulement s'il est multiple de $\operatorname{ppcm}(n, k)$. Or on a $\operatorname{pgcd}(n, k) = 1$, donc $\operatorname{ppcm}(n, k) = nk$.

Les entiers $x$ tels que $x \equiv a[n]$ et $x \equiv b[k]$ sont donc les entiers $x$ tels que $x \equiv x_0[nk]$.

***Second cas*** : $n$ et $k$ ne sont pas premiers entre eux. Posons $d = \operatorname{pgcd}(n, k)$. S'il existe $x \in \mathbb{Z}$ tel que $x \equiv a[n]$ et $x \equiv b[k]$, alors $d$ divise $x - a$ et $x - b$, par suite $d$ divise $(x-b)-(x-a) = a - b$. Si $d$ ne divise pas $a - b$, il n'existe donc pas d'entier $x$ tel que $x \equiv a[n]$ et $x \equiv b[k]$.

Supposons que $d$ divise $a - b$. Notons $n'$ et $k'$ les entiers tels que $n = dn'$ et $k = dk'$. Les entiers $n'$ et $k'$ sont premiers entre eux donc, d'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que $n'u + k'v = 1$.

Posons $x_0 = ak'v + bn'u$. On a $n'u + k'v = 1$ donc $x_0 = a(1 - n'u) + bn'u = a + n'u(b - a)$. On en déduit $x_0 - a = n'u(b - a)$. Or $d$ divise $b - a$ et $n = n'd$, par suite $n$ divise $x_0 - a$, c'est-à-dire $x_0 \equiv a\,[n]$. De même on a $x_0 \equiv b\,[k]$.

Comme dans le premier cas, on en déduit que les entiers $x$ tels que $x \equiv a\,[n]$ et $x \equiv b\,[k]$ sont les entiers $x$ tels que $x \equiv x_0\,[m]$, où $m = \operatorname{ppcm}(n, k)$.



**Exemple 1.** Les entiers 7 et 19 sont premiers entre eux, puisque ce sont des nombres premiers différents. D'après le théorème chinois des restes, il existe $x \in \mathbb{Z}$ tel que $x \equiv 3\,[7]$ et $x \equiv 5\,[19]$. Cherchons tous les entiers $x$ tels que $x \equiv 3[7]$ et $x \equiv 5[19]$.

*Recherche d'une solution particulière.* On a la relation de Bézout $3 \times 19 - 8 \times 7 = 1$, par suite on a

$$\begin{cases} 57 \equiv 1\,[7] \\ 57 \equiv 0\,[19] \end{cases} \quad \text{et} \quad \begin{cases} -56 \equiv 0\,[7] \\ -56 \equiv 1\,[19]. \end{cases}$$

Posons $x_0 = 3 \times 57 - 5 \times 56$. Il vient $x_0 \equiv 3\,[7]$ et $x_0 \equiv 5\,[19]$.

*Recherche de toutes les solutions.* Soit $x \in \mathbb{Z}$. On a $x \equiv 3\,[7]$ et $x \equiv 5\,[19]$ si et seulement si on a $x \equiv x_0\,[7]$ et $x \equiv x_0\,[19]$, c'est-à-dire si et seulement si 7 et 19 divisent $x - x_0$. Puisque 7 et 19 sont premiers, on en déduit que l'on a $x \equiv 3\,[7]$ et $x \equiv 5\,[19]$ si et seulement si $7 \times 19$ divise $x - x_0$.

Mais on a $7 \times 19 = 133$ et $x_0 = -109 = 24 - 133$. Il s'ensuit que les entiers $x$ tels que $x \equiv 3\,[7]$ et $x \equiv 5\,[19]$ sont les entiers $x$ tels que $x \equiv 24\,[133]$.

**Exemple 2.** Les entiers 18 et 45 ne sont pas premiers entre eux : les factorisations de 18 et 45 en produit de nombres premiers sont $18 = 2 \times 3^2$ et $45 = 3^2 \times 5$, donc $\operatorname{pgcd}(18, 45) = 9$. Puisque 9 divise $11 - 2$, il existe $x \in \mathbb{Z}$ tel que $x \equiv 2[18]$ et $x \equiv 11\,[45]$. Cherchons tous les entiers $x$ tels que $x \equiv 2\,[18]$ et $x \equiv 11\,[45]$.

*Recherche d'une solution particulière.* On a la relation de Bézout $5 - 2 \times 2 = 1$. Posons $x_0 = 2 \times 5 - 11 \times 4$, c'est-à-dire $x_0 = -34$. On a $-34 \equiv 2\,[18]$ et $-34 \equiv 11\,[45]$.

*Recherche de toutes les solutions.* Si $x$ est un entier, alors on a $x \equiv 2[18]$ et $x \equiv 11[45]$ si et seulement si $x \equiv x_0\,[18]$ et $x \equiv x_0\,[45]$. On en déduit que les entiers $x$ tels que $x \equiv 2\,[18]$ et $x \equiv 11\,[45]$ sont les entiers $x$ tels que $x \equiv -34\,[\operatorname{ppcm}(18, 45)]$, c'est-à-dire les entiers $x$ tels que $x \equiv -34\,[90]$, ou encore $x \equiv 56\,[90]$.

Les résultats démontrés jusqu'à présent sur les congruences sont une traduction des théorèmes de Bézout et de Gauss. Pour terminer ce chapitre, énonçons un théorème qui simplifie les calculs d'une puissance modulo un nombre premier.

**Petit théorème de Fermat.** *Soit $p$ un nombre premier. Si $x$ est un entier, alors on a $x^p \equiv x\,[p]$.*

**Démonstration.** Pour tout $x \in \mathbb{Z}$, on a $x^2 - x = x(x - 1)$, donc $x^2 - x$ est le produit de deux entiers consécutifs et par suite est pair. Autrement dit, on a $x^2 \equiv x\,[2]$, pour tout $x \in \mathbb{Z}$.

Supposons $p$ impair et démontrons par récurrence que pour tout $x \in \mathbb{N}$, on a $x^p \equiv x\,[p]$. C'est vrai si $x = 0$. Soit $x \in \mathbb{N}$. Supposons que l'on a $x^p \equiv x\,[p]$. D'après la formule du binôme de Newton, on a $(x+1)^p = x^p + C_p^1 x^{p-1} + \cdots + C_p^k x^{p-k} + \cdots + C_p^1 + 1$.

Puisque $p$ est un nombre premier, nous avons vu au paragraphe précédent que pour tout entier $k$ tel que $0 < k < p$, $p$ divise $C_p^k$, c'est-à-dire que l'on a $C_p^k \equiv 0\,[p]$. On en déduit $(x+1)^p \equiv x^p + 1\,[p]$. Mais par hypothèse, nous avons $x^p \equiv x\,[p]$, donc il vient $(x+1)^p \equiv x + 1\,[p]$. Si $x$ est un entier tel que $x < 0$, alors on a $(-x)^p \equiv -x\,[p]$, d'après ce qui précède. En multipliant cette congruence par $(-1)^p = -1$, il vient $x^p \equiv x\,[p]$. ∎

**Corollaire.** *Soit $p$ un nombre premier. Si $x$ n'est pas multiple de $p$, alors on a*

$$x^{p-1} \equiv 1\,[p].$$

**Démonstration.** Soit $x$ un entier non multiple de $p$. D'après le petit théorème de Fermat, $p$ divise $x^p - x = x(x^{p-1} - 1)$. Or $p$ ne divise pas $x$, donc $p$ divise $x^{p-1} - 1$ d'après le lemme d'Euclide. Il s'ensuit $x^{p-1} \equiv 1\,[p]$. ∎

Terminons ce paragraphe par deux exercices où l'on applique le corollaire du petit théorème de Fermat.

**Exercice 1.** Calculer $7^{2003}$ modulo 13.

**Réponse.** Puisque 13 est un nombre premier et que 13 ne divise pas 7, il vient $7^{12} \equiv 1\,[13]$. D'autre part, on a $2003 = 12 \times 166 + 11$ et par suite $7^{2003} = (7^{12})^{166} \times 7^{11}$. Il s'ensuit $7^{2003} \equiv 7^{11}\,[13]$. Enfin, nous avons $7^2 \equiv -3\,[13]$, puis $7^4 \equiv 9\,[13]$, ou encore $7^4 \equiv -4\,[13]$. On en déduit $7^6 \equiv (-3)(-4)\,[13]$. Puisque $7^{11} = 7 \times 7^6 \times 7^4$, il vient $7^{11} \equiv 7(-4)(-1)\,[13]$, ou encore $7^{11} \equiv 2\,[13]$. On a donc $7^{2003} \equiv 2\,[13]$. Le reste de la division euclidienne de $7^{2003}$ par 13 est ainsi égal à 2.

**Exercice 2**

a) Factoriser 1729 en produit de nombres premiers.

b) Soient $a$ et $n$ des entiers positifs. Montrer que l'on a $a^n \equiv 1\,[1729]$ si et seulement si $a^n \equiv 1\,[7]$, $a^n \equiv 1\,[13]$ et $a^n \equiv 1\,[19]$.

c) Soit $a$ un entier positif tel que $\text{pgcd}(a, 1729) = 1$. Démontrer que l'on a $a^{1728} \equiv 1\,[1729]$.

**Réponse**

a) On a $1729 = 7 \times 13 \times 19$.

b) Par définition, on a $a^n \equiv 1\,[1729]$ si et seulement si 1729 divise $a^n - 1$. Puisque 7, 13 et 19 sont des nombres premiers, 1729 divise $a^n - 1$ si et seulement si 7, 13 et 19 divisent $a^n - 1$, d'où le résultat.

c) Puisque $a$ et 1729 sont premiers entre eux, $a$ n'est divisible ni par 7, ni par 13 et ni par 19. On en déduit que l'on a $a^6 \equiv 1\,[7]$, $a^{12} \equiv 1\,[13]$ et $a^{18} \equiv 1\,[19]$. D'autre part on a $1728 = 6 \times 288 = 12 \times 144 = 18 \times 96$, donc $a^{1728} = (a^6)^{288} = (a^{12})^{144} = (a^{18})^{96}$. Par conséquent, il vient $a^{1728} \equiv 1\,[7]$, $a^{1728} \equiv 1\,[13]$ et $a^{1728} \equiv 1\,[19]$. D'après la question précédente, on en déduit $a^{1728} \equiv 1\,[1729]$.





## 6. Un exemple d'application

Pour tout entier positif $n$, nous allons dénombrer les entiers positifs $q$ inférieurs ou égaux à $n$ et premiers avec $n$, c'est-à-dire tels que $q$ et $n$ sont premiers entre eux.

**Définition**

Soit $n$ un entier positif. Le nombre d'entiers compris entre 1 et $n$ et premiers avec $n$ se note $\varphi(n)$. La fonction $\varphi$ ainsi définie s'appelle la *fonction d'Euler*.

**Exemple.**

- Les entiers positifs inférieurs ou égaux à 10 et premiers avec 10 sont 1, 3, 7 et 9 : on a donc $\varphi(10) = 4$.
- On a $\varphi(1) = 1$.
- Soit $p$ un nombre premier. Un entier $a$ est premier avec $p$ si et seulement si $a$ n'est pas multiple de $p$. Par conséquent, tous les entiers positifs strictement inférieurs à $p$ sont premiers avec $p$. Il s'ensuit que si $p$ est un nombre premier, alors $\varphi(p) = p - 1$.
- Soient $p$ un nombre premier et $n$ un entier positif. Tout diviseur positif de $p^n$ est une puissance de $p$. Un entier $a$ est donc premier avec $p^n$ si et seulement si $a$ n'est pas multiple de $p$.

**Proposition.** *Soit $p$ un nombre premier. Pour tout entier $n \geqslant 2$, on a $\varphi(p^n) = p^{n-1}(p-1)$.*

**Démonstration.** Comptons le nombre de multiples de $p$ compris entre 1 et $p^n$. Un multiple de $p$ est de la forme $kp$, où $k$ est un entier. On a $1 \leqslant kp \leqslant p^n$ si et seulement si $1 \leqslant k \leqslant p^{n-1}$, donc il y a $p^{n-1}$ multiples de $p$ compris entre 1 et $p^n$. Puisque $p$ est un nombre premier, un entier $x$ est premier avec $p^n$ si et seulement si $x$ est pas multiple de $p$. On en déduit qu'il y a $p^n - p^{n-1} = p^{n-1}(p-1)$ entiers compris entre 1 et $p^n$ et premiers avec $p$. ∎

Voici la principale propriété de la fonction d'Euler.

**Proposition.** *Soient $a$ et $b$ des entiers positifs. Si $a$ et $b$ sont premiers entre eux, alors $\varphi(ab) = \varphi(a)\varphi(b)$.*

**Démonstration.** On peut supposer $a > 1$. Disposons en tableau tous les entiers compris entre 1 et $ab$, en utilisant $b$ colonnes et $a$ lignes :

| | | | | | |
|---|---|---|---|---|---|
| 1 | 2 | ... | $k$ | ... | $b$ |
| $b+1$ | $b+2$ | ... | $b+k$ | ... | $2b$ |
| $2b+1$ | $2b+2$ | ... | $2b+k$ | ... | $3b$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |
| $mb+1$ | $mb+2$ | ... | $mb+k$ | ... | $(m+1)b$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |
| $(a-1)b+1$ | $(a-1)b+2$ | ... | $(a-1)b+k$ | ... | $ab$ |

Soit $k$ un entier compris entre 1 et $b$ (donc $k$ est situé sur la première ligne du tableau). Pour tout entier $m$, les diviseurs communs à $b$ et $mb+k$ sont les diviseurs communs à $b$ et $k$. On en déduit que si $k$ est premier avec $b$, alors tous les entiers figurant dans sa colonne le sont aussi ; et si $k$ n'est pas premier avec $b$, alors aucun des entiers figurant dans sa colonne n'est premier avec $b$.
Supprimons les colonnes formées d'entiers non premiers avec $b$ : il reste donc $\varphi(b)$ colonnes. Considérons l'une de ces colonnes. Elle est constituée de $a$ entiers $k, b+k, \dots, (a-1)b+k$, tous premiers avec $b$. Posons $E = \{k, b+k, \dots, (a-1)b+k\}$. Faisons l'hypothèse que $a$ et $b$ sont premiers entre eux et pour tout entier $x$, notons $r(x)$ le reste de la division euclidienne de $x$ par $a$. On définit ainsi une application $r : E \to \{0, 1, \dots, a-1\}$.
Supposons que $i$ et $j$ sont des entiers différents compris entre 0 et $a-1$ et que les entiers $ib+k$ et $jb+k$ ont même reste dans la division euclidienne par $a$. Alors on a $ib+k \equiv jb+k\ [a]$, donc $(i-j)b = ib+k-(jb+k)$ est multiple de $a$, autrement dit $a$ divise $(i-j)b$. D'après le théorème de Gauss, on en déduit que $a$ divise l'entier $i-j$, ce qui n'est pas possible car on a $0 < |i-j| \leqslant a-1$. Nous venons de montrer que l'application $r$ est injective.
Puisque l'ensemble de départ et l'ensemble d'arrivée de $r$ sont finis et ont même nombre d'éléments, on en déduit que $r$ est bijective. De plus, un entier $x \in E$ est premier avec $a$ si et seulement si $r(x)$ est premier avec $a$. Or dans l'ensemble $\{0, \dots, a-1\}$, il y a autant d'entiers premiers avec $a$ que dans l'ensemble $\{1, 2, \dots, a\}$, car 0 et $a$ ne sont pas premiers avec $a$. Il s'ensuit que dans l'ensemble $E$, il y a $\varphi(a)$ entiers premiers avec $a$.
Finalement, il y a dans le tableau $\varphi(b)$ colonnes constituées d'entiers premiers avec $b$ et dans chacune, il y a $\varphi(a)$ entiers premiers avec $a$. Parmi les entiers positifs inférieurs ou égaux à $ab$, il y a donc $\varphi(a)\varphi(b)$ entiers premiers avec $a$ et avec $b$. D'après l'exercice page 197, un entier positif est premier avec $ab$ si et seulement s'il est premier avec $a$ et avec $b$. On a donc $\varphi(ab) = \varphi(a)\varphi(b)$. ∎

Les deux propositions précédentes permettent de calculer $\varphi(n)$ connaissant la factorisation de $n$ en nombres premiers.



**Exemples**

- On a $\varphi(3^2 \times 7^3) = \varphi(3^2) \times \varphi(7^3)$ car les entiers $3^2$ et $7^3$ sont premiers entre eux. Puisque 3 et 7 sont des nombres premiers, nous savons que

$$\varphi(3^2) = 3^1(3-1) = 3 \times 2$$
$$\varphi(7^3) = 7^2(7-1) = 7^2 \times 6,$$

donc il vient $\varphi(3^2 \times 7^3) = 3 \times 2 \times 7^2 \times 6 = 2^2 \times 3^2 \times 7^2$.

- Combien y-a-t-il d'entiers positifs inférieurs ou égaux à 2010 et premiers avec 2010 ? On a $2010 = 2 \times 3 \times 5 \times 67$. Puisque 2, 3, 5 et 67 sont des nombres premiers, il vient

$$\varphi(2010) = \varphi(2)\varphi(3)\varphi(5)\varphi(67) = 1 \times 2 \times 4 \times 66 = 528.$$

Il y a donc 528 entiers positifs inférieurs ou égaux à 2010 et premiers avec 2010.

## Exercices

**1.** Soit $n$ un entier supérieur ou égal à 2 et soit $a \in \mathbb{N}$. Soit $P$ le produit des entiers $a+1, a+2, \dots, a+n$. Montrer que $P$ est multiple de $n!$.

**2. a)** Décomposer 8160 en produit de facteurs premiers.
**b)** Trouver tous les entiers positifs $a$ et $b$ tels que $a \geqslant b$, $\text{pgcd}(a, b) = 5$ et $\text{ppcm}(a, b) = 8160$.

**3.** Soient $p$ et $q$ des nombres premiers tels que $p \neq q$. Quels sont les diviseurs positifs de $p^2q$ ?

**4. a)** Montrer qu'un entier impair a tous ses diviseurs impairs.
**b)** Soit $n$ un entier au moins égal à 2. On suppose que tous les diviseurs de $n$ positifs et différents de 1 sont pairs. Montrer que $n$ est une puissance de 2.

**5. a)** Décomposer 2002 en produit de nombres premiers.
**b)** Trouver les nombres premiers compris entre 2001 et 2019.
**c)** Décomposer $\text{ppcm}(2004, 2016)$ en produit de nombres premiers.
**d)** Quel est le nombre de diviseurs positifs de 2016 ?

**6. a)** Soient $b$ et $n$ des entiers supérieurs ou égaux à 2. Montrer que $b^n - 1$ est multiple de $b-1$.
**b)** Soient $a$ et $k$ des entiers supérieurs ou égaux à 2. On suppose que $a^k - 1$ est un nombre premier. Montrer que $a = 2$ et que $k$ est un nombre premier.
**c)** Soit $p$ un nombre premier tel que $p \leqslant 7$. Montrer que $2^p - 1$ est un nombre premier.

**7.** **a)** Calculer $\text{pgcd}(637, 595)$.

**b)** Existe-il des entiers $x$ et $y$ tels que $637x + 595y = 91$ ? Si oui, trouver tous les entiers $x$ et $y$ tels que $637x + 595y = 91$.

**c)** Existe-il des entiers $x$ et $y$ tels que $637x + 595y = 143$ ? Si oui, trouver tous les entiers $x$ et $y$ tels que $637x + 595y = 143$.

**8.** Existe-il des entiers $x$ et $y$ tels que $456057x + 382109y = 7$ ?

**9.** Soient $a$, $b$ et $c$ des entiers positifs. On suppose que $a$ et $c$ sont premiers entre eux.

**a)** Soit $d$ un diviseur de $a$. Montrer que $d$ et $c$ sont premiers entre eux.

**b)** Soit $d$ un diviseur de $a$ et $bc$. Montrer que $d$ divise $b$.

**c)** Montrer que l'on a $\text{pgcd}(a, bc) = \text{pgcd}(a, b)$.

**10.** Trouver tous les entiers $x$ tels que $\begin{cases} 7x \equiv 5\,[19] \\ 3x \equiv 1\,[11]. \end{cases}$

**11.** **a)** Soit $a \in \mathbb{Z}$. Montrer que $a^2$ est congru à 0, 1 ou 4 modulo 8.

**b)** Soient $a, b, c \in \mathbb{Z}$. Montrer que l'entier $1 + a^2 + b^2 + c^2$ n'est pas multiple de 8.

**12.** **a)** Montrer que 223 est un nombre premier.

**b)** Calculer $1998^{1998}$ modulo 223.

**13.** **a)** Factoriser 455 en produit de nombres premiers.

**b)** Soient $a$ et $n$ des entiers naturels. Montrer que l'on a $a^n \equiv 1\,[455]$ si et seulement si $a^n \equiv 1\,[5]$, $a^n \equiv 1\,[7]$ et $a^n \equiv 1\,[13]$.

**c)** Soit $a$ un entier positif tel que $\text{pgcd}(a, 455) = 1$. Montrer que l'on a $a^{12} \equiv 1\,[455]$.

**14.** Trouver trois entiers positifs $a, b, c$ n'ayant que 1 comme diviseur positif commun mais tels que $a$ et $b$ ne sont pas premiers entre eux, $b$ et $c$ non plus, et $a$ et $c$ non plus.

**15.** Soient $x, y, z$ des entiers positifs. On pose $d = \text{pgcd}(\text{pgcd}(x, y), z)$.

**a)** Montrer que $d$ divise $x$, $y$ et $z$.

**b)** Soit $\delta$ un diviseur commun à $x$, $y$ et $z$. Montrer que $\delta$ divise $d$.

**c)** Soient $x'$ le quotient de $x$ par $d$, $y'$ le quotient de $y$ par $d$ et $z'$ le quotient de $z$ par $d$. Montrer que le seul diviseur positif commun à $x'$, $y'$ et $z'$ est égal à 1.



**16.** Soient $a, b, c$ des entiers tels que $2a^2 + b^2 = 5c^2$.

**a)** Montrer que si $a$ et $b$ sont multiples de 5, alors $c$ est multiple de 5.

**b)** On suppose que $a$, $b$ et $c$ ne sont pas tous nuls.

**(i)** Soit $d$ un diviseur positif commun à $a$, $b$ et $c$. Posons $a' = a/d$, $b' = b/d$ et $c' = c/d$. Montrer que l'on a $2a'^2 + b'^2 = 5c'^2$.

**(ii)** Montrer qu'il existe des entiers $a', b', c'$ non tous multiples de 5 et tels que $2a'^2 + b'^2 = 5c'^2$.

**c)** Soit $x \in \mathbb{Z}$. Montrer que $x^2$ est congru à 0, 1 ou 4 modulo 5.

**d)** Montrer que l'on a $(a, b, c) = (0, 0, 0)$.

**17.** Soient $p$ un nombre premier et $a$ un entier positif non multiple de $p$.

**a)** Montrer qu'il existe un plus petit entier positif $k$ tel que $a^k \equiv 1\,[p]$.

**b)** Soit $n \in \mathbb{N}$. Notons $r$ le reste de la division euclidienne de $n$ par $k$. Montrer que l'on a $a^n \equiv a^r\,[p]$.

**c)** Soit $n \in \mathbb{N}$. Montrer que l'on a $a^n \equiv 1\,[p]$ si et seulement si $n$ est multiple de $k$.

**18.** Cet exercice utilise le résultat de l'exercice 17.

**a)** Soit $a$ un entier positif. Montrer que tous les chiffres de $a$ sont égaux à 1 si et seulement s'il existe un entier positif $n$ tel que $9a = 10^n - 1$.

**b)** Soit $n \in \mathbb{N}$. Montrer que l'on a $10^n \equiv 1\,[63]$ si et seulement si $10^n \equiv 1\,[7]$.

**c)** Trouver le plus petit entier positif $k$ tel que $10^k \equiv 1\,[7]$.

**d)** En déduire que 111111 est le plus petit multiple de 7 dont tous les chiffres sont égaux à 1.

**19.** Cet exercice utilise le résultat de l'exercice 17.

**a)** Démontrer que l'on a $5^8 \equiv -1\,[17]$.

**b)** En déduire que 16 est le plus petit entier positif $k$ tel que $5^k \equiv 1\,[17]$.

**c)** Soit $a$ un entier tel que $1 \leqslant a \leqslant 16$. Montrer qu'il existe $n \in \mathbb{N}$ tel que $5^n \equiv a\,[17]$.

**d)** Trouver tous les entiers naturels $n$ tels que $5^n \equiv 3\,[17]$.

**20.** Cet exercice utilise le résultat de l'exercice 17.

**a)** Soit $p$ un facteur premier de $2^{11} - 1$. Montrer que 11 est le plus petit entier positif $k$ tel que $2^k \equiv 1\,[p]$. En déduire que 22 divise $p - 1$.

**b)** Calculer $2^{11}$ modulo 23. En déduire que $2^{11} - 1$ n'est pas un nombre premier.

**21.** Cet exercice utilise le résultat de l'exercice 17.

**a)** Soit $p$ un facteur premier de $2^{13}-1$. Montrer que 13 est le plus petit entier positif $k$ tel que $2^k \equiv 1\,[p]$. En déduire que $p$ est congru à 1 modulo 26.

**b)** Montrer que les nombres premiers plus petits ou égaux à $\sqrt{2^{13}-1}$ et congrus à 1 modulo 26 sont 53 et 79.

**c)** Calculer $2^{13}$ modulo 53 et modulo 79.

**d)** Montrer que $2^{13}-1$ est un nombre premier.

**22. a)** Soit $n$ un entier plus grand ou égal à 2 tel que $n \equiv 3\,[4]$. Montrer que pour tout facteur premier $p$ de $n$, on a $p \equiv 1\,[4]$ ou $p \equiv 3\,[4]$. En déduire qu'il existe un facteur premier $p$ de $n$ congru à 3 modulo 4.

**b)** Soit $k$ un entier positif. Supposons que $p_1, \dots, p_k$ sont des nombres premiers congrus à 3 modulo 4 et considérons l'entier $n = 4p_1 \cdots p_k - 1$. Montrer que l'on a $n \geqslant 2$ et qu'il existe un facteur premier $p$ de $n$ congru à 3 modulo 4. Montrer que $p$ est différent de tous les $p_i$.

**c)** Démontrer qu'il existe une infinité de nombres premiers congrus à 3 modulo 4.

**23. a)** Soit $N$ un entier plus grand ou égal à 2. Posons $n = (N!)^2 + 1$ et considérons $p$ un facteur premier de $n$. Montrer que $p$ est impair, que $p$ ne divise pas $N!$ et que l'on a $(N!)^2 \equiv -1\,[p]$. En déduire que $(-1)^{\frac{p-1}{2}} \equiv 1\,[p]$ puis $p \equiv 1\,[4]$.

**b)** Montrer que pour tout entier $N$ supérieur ou égal à 2, il existe un nombre premier $p$ congru à 1 modulo 4 tel que $p > N$. En déduire qu'il existe une infinité de nombres premiers congrus à 1 modulo 4.

**24.** Calculer le nombre d'entiers positifs inférieurs ou égaux à 756 et premiers avec 756.

**25.** Soient $p$ un nombre premier, $m$ un entier positif et $a$ un entier positif tel que $a \equiv 1\,[p^m]$. Montrer que $a^p \equiv 1\,[p^{m+1}]$.

**26.** Cet exercice utilise le résultat de l'exercice 25.

Soient $n$ un entier au moins égal à 2 et $a$ un entier positif tel que $a$ et $n$ soient premiers entre eux. Soit $p$ un facteur premier de $n$.

**a)** Montrer que $a$ n'est pas multiple de $p$.

**b)** Montrer que $a^{p(p-1)} \equiv 1\,[p^2]$.

**c)** Soit $k$ un entier positif. Montrer que $a^{p^k(p-1)} \equiv 1\,[p^{k+1}]$.

**d)** Soit $m$ l'exposant de $p$ dans $n$. Montrer que $a^{\varphi(n)} \equiv 1\,[p^m]$.

**e)** Montrer que $a^{\varphi(n)} \equiv 1\,[n]$.



## Quelques réponses ou indications

1. On a $(a!)P = (a+n)!$ et $(a!)(n!)C_n^a = (a+n)!$, où $C_n^a$ est le coefficient binomial.

2. b) Il y a quatre solutions.

3. Il y a six diviseurs positifs.

4. b) Considérer la décomposition de $n$ en facteurs premiers.

5. b) Il y a deux nombres premiers entre 2001 et 2019 : ce sont les entiers 2011 et 2017.
c) $\mathrm{ppcm}(2004, 2016) = 2^5 \times 3^2 \times 7 \times 167$.
d) L'entier 2016 possède 36 diviseurs positifs.

6. a) On a $b^n - 1 = (b-1)(b^{n-1} + \cdots + b + 1)$.
b) Il faut appliquer deux fois le résultat de la question précédente : une première fois avec $b = a$ et une seconde fois avec $b = a^d$, où $d$ est un diviseur de $k$ supérieur ou égal à 2.

8. On a $\mathrm{pgcd}(456057, 382109) = 133$ et la réponse est non.

9. b) D'après (a), les entiers $d$ et $c$ sont premiers entre eux. Puisque $d$ divise $bc$, $d$ divise $b$ d'après le théorème de Gauss.
c) Montrer que $\mathrm{pgcd}(a,b)$ divise $\mathrm{pgcd}(a,bc)$ et utiliser (b) pour montrer que $\mathrm{pgcd}(a,bc)$ divise $\mathrm{pgcd}(a,b)$.

10. La réponse est $x \equiv -40\,[209]$.

12. b) On a $1998^{1998} \equiv 1\,[223]$ car 1998 est multiple de 222.

13. c) Puisque $a$ et 455 sont premiers entre eux, $a$ n'est divisible ni par 5, ni par 7 et ni par 13. On a donc $a^4 \equiv 1\,[5]$, $a^6 \equiv 1\,[7]$ et $a^{12} \equiv 1\,[13]$.

15. b) c) Utiliser la proposition page 195.

16. b) (ii) Considérer le plus grand entier $k$ tel que $5^k$ divise $a$, $b$ et $c$ et appliquer (i).
d) D'après (a) et (b) (ii), les entiers $a'$ et $b'$ ne sont pas tous les deux multiples de 5. Quelles sont les congruences modulo 5 possibles pour l'entier $2a'^2 + b'^2$ ?

17. a) Utiliser le corollaire du petit théorème de Fermat.
b) Si $n = ku + r$, alors $a^n = (a^k)^u a^r$.

18. c) Puisque 7 ne divise pas 10, on a $10^6 \equiv 1\,[7]$. D'après l'exercice 11, le plus petit entier positif $k$ tel que $10^k \equiv 1\,[7]$ est un diviseur de 6.

19. d) La réponse est $n \equiv 13\,[16]$.

20. a) Puisque $2^{11} \equiv 1\,[p]$, $p$ est impair. D'après l'exercice 11, le plus petit entier positif $k$ tel que $2^k \equiv 1\,[p]$ est un diviseur de 11, par suite est égal à 1 ou 11. Or 2 n'est pas congru à 1 modulo 11 par conséquent 11 est le plus petit entier positif $k$ tel que $2^k \equiv 1\,[p]$. Puisque $2^{p-1} \equiv 1\,[p]$, 11 divise $p-1$. Et comme $p-1$ est pair, 22 divise $p-1$.

21. **a)** Comme dans l'exercice précédent, on démontre que 26 divise $p-1$, ce qui veut exactement dire que $p$ est congru à 1 modulo 26.

**d)** Si $2^{13}-1$ n'était pas un nombre premier, alors $2^{13}-1$ aurait un facteur premier plus petit ou égal à $\sqrt{2^{13}-1}$. En déduire une contradiction.

22. **a)** L'entier $n$ est impair, donc tous ses diviseurs le sont. Par ailleurs, un produit d'entiers congrus à 1 modulo 4 est congru à 1 modulo 4.

**b)** Si $p$ était égal à l'un des $p_i$, l'entier $4p_1 \cdots p_k - n$ serait multiple de $p$.

**c)** Utiliser (b).

23. **a)** On a $(-1)^{\frac{p-1}{2}} \equiv (N!)^{p-1}\,[p]$.

**b)** Un entier qui ne divise pas $N!$ est strictement plus grand que $N$.

25. Il existe un entier $k$ tel que $a = 1 + kp^m$. Exprimer $a^p$ selon la formule du binôme de Newton et se rappeler que pour tout entier $i$ tel que $0 < i < p$, l'entier $C_p^i$ est multiple de $p$. Remarquer enfin que $(p^m)^p$ est multiple de $p^{m+1}$.

26. **b)** D'après le corollaire du petit théorème de Fermat, on a $a^{p-1} \equiv 1\,[p]$.

**c)** Raisonner par récurrence.

**d)** Puisque $\varphi(n)$ est multiple de $\varphi(p^m)$, il suffit de montrer que l'on a $a^{\varphi(p^m)} \equiv 1\,[p^m]$.

**e)** Considérer la décomposition de $n$ en facteurs premiers. Le résultat de cet exercice généralise le corollaire du petit théorème de Fermat.



# Chapitre 10

# Polynômes

Dans ce chapitre, la lettre $\mathbf{K}$ désigne $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$. Nous allons définir ce qu'est un *polynôme à coefficients dans* $\mathbf{K}$. À chaque fois que nous écrirons « polynôme », cela voudra dire polynôme à coefficients dans $\mathbf{K}$. Vous constaterez la similitude des énoncés des paragraphes 2, 3, 4 et 6 de ce chapitre avec les paragraphes correspondants du chapitre précédent. Lorsque la démonstration d'un énoncé sera en tout point identique à celle donnée en arithmétique, nous ne la reproduirons pas dans ce chapitre sur les polynômes.

## 1. Définitions et règles de calcul

**Définition**

Un *polynôme à coefficients dans* $\mathbf{K}$ est une suite $(a_n)$ de nombres appartenant à $\mathbf{K}$, telle qu'il existe un entier $p \in \mathbb{N}$ vérifiant $a_n = 0$ pour tout entier $n > p$.

Un polynôme est noté avec une lettre capitale, par exemple $P$, mais aussi $Q$ ou $A$. Un exemple de polynôme est la suite dont tous les termes sont nuls. Ce polynôme s'appelle le polynôme nul.

Par définition, si $P$ et $Q$ sont les polynômes $(a_n)$ et $(b_n)$, on a $P=Q$ si et seulement si $a_n = b_n$ pour tout $n \in \mathbb{N}$.

### Opérations sur les polynômes

Si $P$ est le polynôme $(a_n)$, si $Q$ est le polynôme $(b_n)$ et si $\lambda \in \mathbf{K}$, alors les suites $(\lambda a_n)$, $(a_n + b_n)$ et $(a_n - b_n)$ sont des polynômes. En effet, si $a_n = 0$ pour tout entier $n > p$, alors $\lambda a_n = 0$ pour tout entier $n > p$. De plus, si $b_n = 0$ pour tout entier $n > q$, alors $a_n + b_n = 0$ et $a_n - b_n = 0$ pour tout entier $n > \max(p,q)$. On définit alors

- la multiplication de $P$ par le scalaire $\lambda$ en posant $\lambda P = (\lambda a_n)$
- la somme et la différence des polynômes $P$ et $Q$ en posant $P + Q = (a_n + b_n)$ et $P - Q = (a_n - b_n)$.

Nous allons maintenant définir le produit de deux polynômes. Mais attention, contrairement aux opérations précédentes, le produit de deux polynômes n'est pas le produit de deux suites défini en analyse. Pour formuler cette définition, démontrons un résultat préalable.

**Lemme.** *Soient $(a_n)$ et $(b_n)$ des polynômes et soit $(c_n)$ la suite définie par $c_0 = a_0b_0$ et $c_n = a_0b_n + \cdots + a_kb_{n-k} + \cdots + a_nb_0$ pour tout entier positif $n$. Alors la suite $(c_n)$ est un polynôme.*

**Démonstration.** Puisque les suites $(a_n)$ et $(b_n)$ sont des polynômes, il existe un entier $p \in \mathbf{N}$ tel que $a_n = 0$ pour tout entier $n > p$ et il existe un entier $q \in \mathbf{N}$ tel que $b_n = 0$ pour tout entier $n > q$. Soit $n$ un entier tel que $n > p + q$. Pour tout entier $k$ tel que $0 \leqslant k \leqslant n$, on a $k > p$ ou $n - k > q$, donc $a_kb_{n-k} = 0$. On en déduit $c_n = 0$. ∎

**Définition**

Soient $P$ et $Q$ les polynômes $(a_n)$ et $(b_n)$. Le polynôme $(c_n)$ défini dans le lemme ci-dessus s'appelle le *produit* de $P$ par $Q$ et se note $PQ$.

Faisons quelques calculs de produit sur des polynômes très simples. Pour tout entier naturel $p$, définissons le polynôme $E_p$ comme étant la suite $(a_n)$ telle que $a_p = 1$ et $a_n = 0$ pour tout entier $n \neq p$.

- Par exemple, on a $E_2E_3 = E_5$ et pour tout $p \in \mathbf{N}$, $E_1E_p = E_{p+1}$.
- Si $P$ est un polynôme, alors $E_0P = P$ et plus généralement on a l'égalité $(aE_0)P = aP$ pour tout $a \in \mathbf{K}$.

Cette dernière égalité permet de noter simplement $a$ le polynôme $aE_0$. Nous venons ainsi de convenir que $\mathbf{K}$ est inclus dans l'ensemble des polynômes à coefficients dans $\mathbf{K}$. Un élément de $\mathbf{K}$ s'appelle un polynôme *constant*.

### Règles de calcul

Muni des deux opérations somme et multiplication par un élément de $\mathbf{K}$, l'ensemble des polynômes à coefficients dans $\mathbf{K}$ est un $\mathbf{K}$-espace vectoriel. Autrement dit, pour tous polynômes $P, Q, R$ à coefficients dans $\mathbf{K}$ et pour tous $a, b \in \mathbf{K}$, nous avons

$$(P+Q)+R = P+(Q+R) \quad \text{et ce polynôme est noté } P+Q+R,$$
$$P+Q = Q+P, \quad P+0 = P, \quad P-P = 0, \quad 1P = P,$$
$$a(P+Q) = aP + aQ, \quad (a+b)P = aP + bP,$$
$$a(bP) = (ab)P \quad \text{et ce polynôme est noté } abP.$$





En ce qui concerne le produit des polynômes, on a pour tous polynômes $P, Q, R$ à coefficients dans $\mathbf{K}$,

$$PQ = QP, \quad P(Q+R) = PQ + PR,$$
$$P(QR) = (PQ)R \quad \text{et ce polynôme est noté } PQR.$$

Toutes ces règles se vérifient en utilisant la définition des opérations.

**Notation.** Soit $P$ un polynôme. On pose $P^0 = 1$ et pour tout entier positif $n$, on note $P^n$ le produit de $P^{n-1}$ par $P$.

En utilisant les règles de calcul et les propriétés des coefficients binômiaux, on démontre comme dans $\mathbf{C}$ la formule du binôme de Newton :

- pour tous polynômes $P$ et $Q$ et pour tout entier positif $n$, on a

$$(P+Q)^n = P^n + C_n^1P^{n-1}Q + \cdots + C_n^kP^{n-k}Q^k + \cdots + C_n^{n-1}PQ^{n-1} + Q^n.$$

**Exemple.** Soient $P$ et $Q$ des polynômes. Il vient

$$(P+Q)^2 = P^2 + 2PQ + Q^2 \quad \text{et} \quad (P-Q)^3 = P^3 - 3P^2Q + 3PQ^2 - Q^3.$$

**Définition**

Soit $P = (a_k)$ un polynôme non nul. Le plus grand entier $n$ tel que $a_n \neq 0$ s'appelle le *degré* de $P$ et se note $\deg P$.

**Exemple.** Soit $P$ un polynôme non nul. Alors le polynôme $P$ est constant si et seulement si $\deg P = 0$.

**Notations.** Notons $X$ le polynôme $E_1$, c'est-à-dire la suite $(a_k)$ définie par $a_1 = 1$ et $a_k = 0$ pour tout entier $k \neq 1$ et notons $\mathbf{K}[X]$ l'ensemble des polynômes à coefficients dans $\mathbf{K}$.

**Proposition.** *Soit $P$ un polynôme de $\mathbf{K}[X]$, non constant et de degré $n$. Alors il existe des éléments uniques $a_0, \ldots, a_n$ appartenant à $\mathbf{K}$, tels que $a_n \neq 0$ et $P = a_nX^n + \cdots + a_1X + a_0$.*

**Démonstration.** Notons $(b_k)$ le polynôme $P$. Puisque $P$ est de degré $n$, on a $b_n \neq 0$ et $b_k = 0$ pour tout entier $k > n$. Reprenons les polynômes $E_p$ : $E_p$ est la suite $(c_k)$ telle que $c_p = 1$ et $c_k = 0$ pour tout entier $k \neq p$. Par définition des opérations somme et multiplication par un scalaire, on a $P = b_nE_n + \cdots + b_1E_1 + b_0$. De plus, si $P = a_qE_q + \cdots + a_1E_1 + a_0$, alors on a $P = (a_k)$, où l'on a posé $a_k = 0$ pour tout entier $k > q$. Par définition de $n$, on en déduit $q \geqslant n$ et $a_k = 0$ si $n < k \leqslant q$. On a donc $a_k = b_k$ pour tout $k$.

On vient donc de démontrer que $P$ s'écrit de manière unique comme combinaison linéaire de $E_0, E_1, \ldots, E_n$. Enfin, puisque $E_1 E_p = E_{p+1}$ pour tout $p \in \mathbb{N}$, on démontre par récurrence que pour tout $p \in \mathbb{N}$, on a $E_1^p = E_p$, c'est-à-dire $E_p = X^p$, d'où le résultat. ∎

**Définition**

Soit $P = a_n X^n + \cdots + a_0$ un polynôme non nul de degré $n$. Alors $a_n$ s'appelle le coefficient *dominant* de $P$ et $a_n X^n$ s'appelle le *monôme de plus haut degré* de $P$. Si $a_n = 1$, on dit que le polynôme $P$ est *unitaire*.

**Exemples de calcul sur les polynômes**

1) Pour tous polynômes $P$ et $Q$, on a $P^2 - Q^2 = (P-Q)(P+Q)$.
En effet, les règles de calcul sur les polynômes permettent d'écrire les égalités

$$(P-Q)(P+Q) = P(P+Q) - Q(P+Q) = P^2 + PQ - QP - Q^2 = P^2 - Q^2.$$

2) Soient $A$, $P$ et $Q$ les polynômes suivants de $\mathbb{Q}[X]$ :

$$A = X^7 + X^6 + X^5 - 3X^4 + 11X^3 + 11X^2 + 15X - 12$$

$$P = X^3 + X^2 + X - 1 \quad \text{et} \quad Q = X^4 - 2X + 13.$$

Calculer $P+Q$ est très facile : on ajoute coefficient par coefficient. Il vient

$$P + Q = X^4 + X^3 + X^2 - X + 12.$$

Pour calculer $PQ$, on utilise les règles de calculs comme suit :

$$\begin{aligned} PQ &= (X^3 + X^2 + X - 1)(X^4 - 2X + 13) \\ &= X^4(X^3 + X^2 + X - 1) - 2X(X^3 + X^2 + X - 1) + 13(X^3 + X^2 + X - 1) \\ &= (X^7 + X^6 + X^5 - X^4) - 2(X^4 + X^3 + X^2 - X) + 13(X^3 + X^2 + X - 1) \\ &= X^7 + X^6 + X^5 - 3X^4 + 11X^3 + 11X^2 + 15X - 13. \end{aligned}$$

Enfin, pour calculer $A - PQ$, on retranche coefficient par coefficient et l'on obtient $A - PQ = 1$.

**Remarque**

Soit $n$ un entier positif. D'après la proposition précédente, l'ensemble $E$ des polynômes de $\mathbf{K}[X]$ nul ou de degré inférieur ou égal à $n$ est un sous-espace vectoriel de $\mathbf{K}[X]$ de dimension $n+1$ : en effet, $(1, X, \ldots, X^n)$ est une base de $E$.
De manière générale, si $P_i$ est un polynôme de degré $i$, alors $(P_0, P_1, \ldots, P_n)$ est une base de $E$. Pour le montrer, supposons que $\lambda_0, \lambda_1, \ldots, \lambda_n$ sont des éléments de $\mathbf{K}$ tels que $\lambda_0 P_0 + \lambda_1 P_1 + \cdots + \lambda_n P_n = 0$. Notons $a_i$ le coefficient dominant du polynôme $P_i$, pour tout $i \in \{0, 1, \ldots, n\}$. Puisque le polynôme $P_i$ est de degré $i$, le coefficient de $X^n$ dans le polynôme $\lambda_0 P_0 + \lambda_1 P_1 + \cdots + \lambda_n P_n$ est $a_n \lambda_n$. Puisque ce polynôme est nul, on en déduit $\lambda_n = 0$ et par suite $\lambda_0 P_0 + \cdots + \lambda_{n-1} P_{n-1} = 0$. On démontre alors par récurrence sur $k$ que pour tout entier $k \in \{0, 1, \ldots, n\}$, on a $\lambda_{n-k} = 0$. Les vecteurs $P_0, P_1, \ldots, P_n \in E$ sont donc linéairement indépendants. Puisque $\dim E = n+1$, on en déduit que $(P_0, P_1, \ldots, P_n)$ est une base de $E$.



**Exemple.** Les polynômes $1$, $X$, $X(X-1)$ $X(X-1)(X-2)$ forment une base de l'espace vectoriel des polynômes nul ou de degré inférieur ou égal à 3.

**Proposition.** *Soient $P$ et $Q$ des polynômes non nuls de $\mathbf{K}[X]$.*
- *Le polynôme $PQ$ est non nul et $\deg(PQ) = \deg P + \deg Q$.*
- *Si $P+Q$ n'est pas le polynôme nul, alors $\deg(P+Q) \leqslant \max(\deg P, \deg Q)$.*
- *Si $\deg P \neq \deg Q$, alors $P + Q \neq 0$ et $\deg(P+Q) = \max(\deg P, \deg Q)$.*

**Démonstration.** Posons $p = \deg P$ et $q = \deg Q$, $P = a_p X^p + \cdots + a_1 X + a_0$ et $Q = b_q X^q + \cdots + b_1 X + b_0$. On a donc $a_p \neq 0$ et $b_q \neq 0$. Il vient

$$PQ = a_p b_q X^{p+q} + (a_p b_{q-1} + a_{p-1} b_q) X^{p+q-1} + \cdots + (a_1 b_0 + a_0 b_1) X + a_0 b_0.$$

Puisque $a_p b_q \neq 0$, le polynôme $PQ$ est non nul et de degré $p+q$.
Posons $n = \max(\deg P, \deg Q)$, $a_k = 0$ pour tout entier $k > p$ et $b_\ell = 0$ pour tout entier $\ell > q$. Il vient $P + Q = (a_n + b_n) X^n + \cdots + (a_1 + b_1) X + a_0 + b_0$. Il est donc clair que si $P+Q$ n'est pas le polynôme nul, alors on a $\deg(P+Q) \leqslant n$. De plus, si $p > q$ par exemple, alors $n = p$ et $a_n + b_n = a_p$ ; il s'ensuit $\deg(P+Q) = n$. ∎

**Corollaire.** *Soit $P$ un polynôme non nul. Si $Q$ et $R$ sont des polynômes tels que $PQ = PR$, alors $Q = R$.*

**Démonstration.** Supposons $PQ = PR$. Il vient $P(Q-R) = 0$. Si $Q - R$ n'était pas le polynôme nul, le polynôme $P(Q-R)$ ne serait pas nul, d'après la proposition précédente. Il s'ensuit $Q - R = 0$, c'est-à-dire $Q = R$. ∎

**Définition**

Soit $P$ un polynôme de $\mathbf{K}[X]$. Le *polynôme dérivé* de $P$, noté $P'$, est le polynôme de $\mathbf{K}[X]$ défini en posant $P' = 0$ si $P$ est un polynôme constant et $P' = n a_n X^{n-1} + (n-1) a_{n-1} X^{n-2} + \cdots + a_1$ s'il existe un entier positif $n$ tel que $P = a_n X^n + \cdots + a_1 X + a_0$ et $a_n \neq 0$.

**Exemples**
- Si $n$ est un entier positif, le polynôme dérivé de $X^n$ est $nX^{n-1}$.
- Le polynôme dérivé de $X^2 + aX + b$ est $2X + a$.

Les propriétés énoncées dans le lemme suivant sont immédiates.

**Lemme.** *Soient $P$ et $Q$ des polynômes de $\mathbf{K}[X]$ et $\lambda$ un élément de $\mathbf{K}$. Alors on a $(P+Q)' = P' + Q'$, $(\lambda P)' = \lambda P'$ et $(PQ)' = P'Q + PQ'$.*

En particulier, l'application de $\mathbf{K}[X]$ dans $\mathbf{K}[X]$ qui à tout polynôme $P$ associe $P'$ est linéaire. Remarquons que les règles pour calculer un polynôme dérivé sont les mêmes que les règles de dérivation des fonctions.

Terminons ce paragraphe en introduisant la notion de *composé* de polynômes, notion notamment utile en analyse pour calculer le développement limité d'une composée de fonctions.

**Définition**

Soient $P$ et $Q$ des polynômes. Le polynôme *composé* de $P$ et $Q$, noté $P \circ Q$, est défini de la manière suivante : si $P$ est constant, alors $P \circ Q = P$ et s'il existe un entier positif $n$ tel que $P = a_n X^n + \cdots + a_1 X + a_0$ et $a_n \neq 0$, alors $P \circ Q = a_n Q^n + \cdots + a_1 Q + a_0$.

Si par exemple $Q = X^2$, par commodité on note $P(X^2)$ le polynôme $P \circ Q$. Ainsi lorsque $P = X^3 - X + 1$, nous avons $P(X^2) = X^6 - X^2 + 1$.

## 2. Divisibilité

**Définition**

Soient $A$ et $B$ des polynômes. On dit que $A$ *divise* $B$, ou que $A$ est un *diviseur* de $B$, ou encore que $B$ est *multiple* de $A$ s'il existe un polynôme $Q$ tel que $B = AQ$.

**Exemples**

- Tout polynôme divise 0, c'est-à-dire tout polynôme divise le polynôme nul.
- Le seul multiple de 0 est 0.
- Soient $P$ un polynôme non nul et $a$ un élément non nul de $\mathbf{K}$. Alors $aP$ et $a$ sont des diviseurs de $P$.
- Le polynôme $X^5 + X + 1$ est multiple de $X^2 + X + 1$.
- Pour tout entier positif $n$, $X - 1$ divise $X^n - 1$. Par exemple, on a

$$X^3 - 1 = (X-1)(X^2 + X + 1) \quad \text{et} \quad X^4 - 1 = (X-1)(X^3 + X^2 + X + 1).$$

**Lemme.** *Soient $A$ et $B$ des polynômes. Si $B$ n'est pas le polynôme nul et si $A$ divise $B$, alors il existe un unique polynôme $Q$ tel que $B = AQ$.*





**Lemme.** *Soient $P$ et $Q$ des polynômes tous deux non nuls. Si $P$ divise $Q$, alors $\deg P \leqslant \deg Q$.*

**Démonstration.** Supposons qu'il existe un polynôme $R$ tel que $Q = PR$. Puisque $Q$ n'est pas nul, on a $R \neq 0$ et $\deg Q = \deg P + \deg R$, d'où le résultat. ∎

En particulier, les seuls diviseurs du polynôme constant égal à 1 sont les polynômes constants non nuls.

**Lemme.** *Soient $A, B, C$ des polynômes non nuls.*

- *Si $A$ divise $B$ et si $B$ divise $C$, alors $A$ divise $C$.*
- *Si $A$ divise $B$ et si $B$ divise $A$, alors il existe un élément non nul $\lambda$ de $\mathbf{K}$ tel que $B = \lambda A$.*
- *Si $A$ divise $B$ et si $A$ divise $C$, alors $A$ divise $B + C$.*

**Démonstration.** Soient $A$ et $B$ des polynômes non nuls tels que $A$ divise $B$ et $B$ divise $A$. Puisque $B$ divise $A$ et que $A$ est non nul, il existe un polynôme non nul $Q$ tel que $A = BQ$. Il vient $\deg A = \deg B + \deg Q$. Puisque $A$ divise $B$, on a l'inégalité $\deg A \leqslant \deg B$. Il s'ensuit $\deg Q = 0$. Le polynôme $Q$ est donc constant. Les deux autres propriétés se démontrent comme en arithmétique. ∎

**Proposition.** *Soit $B$ un polynôme non nul. Si $A$ est un polynôme, alors il existe des polynômes $Q$ et $R$ uniques tels que $A = BQ + R$ et $R = 0$ ou bien $\deg R < \deg B$.*

**Démonstration.** Si $A = 0$, il suffit de prendre $Q = 0$ et $R = 0$. Si $B$ est le polynôme constant égal à $b$, il suffit de prendre $Q = \frac{1}{b}A$ et $R = 0$. Supposons $A \neq 0$, $B$ non constant et démontrons l'existence des polynômes $Q$ et $R$ par récurrence sur le degré de $A$. Si l'on a $\deg A < \deg B$, ce qui est possible puisque $\deg B \geqslant 1$, il suffit de prendre $Q = 0$ et $R = A$.

Si $\deg A \geqslant \deg B$, posons $n = \deg A$, $p = \deg B$, notons $a$ le coefficient dominant de $A$ et $b$ celui de $B$. Écrivons $A = aX^n + U$ et $B = bX^p + C$ ; il vient $U = 0$ ou $\deg U < n$ et de même $C = 0$ ou $\deg C < p$. Par hypothèse de récurrence, il existe des polynômes $Q_1$ et $R_1$ tels que $U = BQ_1 + R_1$ et $R_1 = 0$ ou $\deg R_1 < p$. D'autre part on a

$$aX^n = \frac{a}{b}X^{n-p}(bX^p) = \frac{a}{b}X^{n-p}(B - C) = \frac{a}{b}X^{n-p}B - \frac{a}{b}X^{n-p}C.$$

Le degré d'un produit de polynômes étant la somme des degrés, on en déduit $-\frac{a}{b}X^{n-p}C = 0$ ou $\deg\left(-\frac{a}{b}X^{n-p}C\right) = n - p + \deg C < n$. Par hypothèse de récurrence, il existe des polynômes $Q_2$ et $R_2$ tels que

$$-\frac{a}{b}X^{n-p}C = BQ_2 + R_2 \quad \text{et} \quad R_2 = 0 \quad \text{ou} \quad \deg R_2 < p.$$

Finalement, on obtient

$$A = aX^n + U = \frac{a}{b}X^{n-p}B + BQ_2 + R_2 + BQ_1 + R_1 = B\left(\frac{a}{b}X^{n-p} + Q_2 + Q_1\right) + (R_2 + R_1).$$

Si $R_1 \neq 0$ et $R_2 \neq 0$, alors $R_1 + R_2 = 0$ ou $\deg(R_1 + R_2) \leqslant \max(\deg R_1, \deg R_2) < p$. Dans tous les cas, on a donc $R_1 + R_2 = 0$ ou $\deg(R_1 + R_2) < p$, ce qui achève la démonstration de l'existence.

Démontrons l'unicité de ces polynômes. Soient $Q_1$ et $R_1$ vérifiant les conditions de la proposition, ainsi que $Q_2$ et $R_2$. Il vient $B(Q_1 - Q_2) = R_2 - R_1$. Raisonnons par l'absurde en supposant que le polynôme $Q_1 - Q_2$ n'est pas nul. Alors le polynôme $R_2 - R_1$ n'est pas nul et l'on a $\deg(R_2 - R_1) = \deg B + \deg(Q_1 - Q_2)$, donc $\deg(R_2 - R_1) \geqslant \deg B$, puisque $\deg(Q_1 - Q_2)$ est un entier positif ou nul. D'autre part, si $R_1 = 0$ ou si $R_2 = 0$, il vient $R_2 - R_1 = R_2$ ou $R_2 - R_1 = -R_1$ et il s'ensuit $\deg(R_2 - R_1) < \deg B$, ce qui est contradictoire. Enfin, si $R_1 \neq 0$ et $R_2 \neq 0$, alors $\deg(R_2 - R_1) \leqslant \max(\deg R_1, \deg R_2)$ et par suite $\deg(R_2 - R_1) < \deg B$, ce qui est à nouveau une contradiction. ■

**Définition**

Dans la proposition ci-dessus, le polynôme $Q$ s'appelle le *quotient* et le polynôme $R$ s'appelle le *reste de la division euclidienne* de $A$ par $B$.

Soient $A$ un polynôme et $B$ un polynôme non nul. D'après l'unicité énoncée dans la proposition ci-dessus, $B$ divise $A$ si et seulement si le reste de la division euclidienne de $A$ par $B$ est nul et dans ce cas, le quotient de la division euclidienne de $A$ par $B$ s'appelle plus simplement le quotient de $A$ par $B$.

**Remarque**

Soit $R$ le reste de la division euclidienne de $A$ par $B$. Si $P$ est un polynôme, alors $P$ divise $A$ et $B$ si et seulement si $P$ divise $B$ et $R$. Pour démontrer ce résultat, on raisonne comme dans la démonstration de la proposition page 192.

Pour faire la division euclidienne de $A$ par $B$ lorsque $\deg A \geqslant \deg B$, on procède comme dans la démonstration, c'est-à-dire que l'on divise le monôme de plus haut degré de $A$ par le monôme de plus haut degré de $B$. On écrit ce qu'il reste et l'on poursuit cette opération jusqu'à obtenir un polynôme nul ou de degré plus petit que celui de $B$.

**Exemple 1.** Au début de ce paragraphe, nous avons énoncé que $X^5 + X + 1$ est multiple de $X^2 + X + 1$. Un moyen de le démontrer est de prouver que le reste de la division euclidienne de $A = X^5 + X + 1$ par $B = X^2 + X + 1$ est nul. Faisons cette division. Le monôme de plus haut degré de $A$ est $X^5$, celui de $B$ est $X^2$ et l'on a $X^5 = X^2X^3$. Écrivons donc $A = X^5 + X + 1 = (X^2 + X + 1)X^3 + A_1$. Il vient

$$A_1 = X^5 + X + 1 - (X^5 + X^4 + X^3) = -X^4 - X^3 + X + 1.$$

Le polynôme $A_1$ étant de degré plus grand que celui de $B$, on divise par $X^2$ son monôme de plus haut degré : $-X^4 = X^2(-X^2)$. Nous obtenons

$$\begin{aligned} A_1 &= (X^2 + X + 1)(-X^2) + A_2 \quad \text{où} \quad A_2 = X^2 + X + 1 \\ &= (X^2 + X + 1)(-X^2 + 1). \end{aligned}$$

Puisque $A = (X^2 + X + 1)X^3 + A_1$, il s'ensuit $A = (X^2 + X + 1)(X^3 - X^2 + 1)$.

**Exemple 2.** Calculons le quotient et le reste de la division euclidienne de $X^5 + X^2 + 1$ par $X^2 + X + 1$. Il est commode de disposer les calculs comme suit.

$$\begin{array}{rl|l} & X^5 + \qquad\qquad + X^2 + \quad + 1 & X^2 + X + 1 \\ - & X^5 + X^4 + X^3 & \overline{X^3 - X^2 + 2} \\ \hline & -X^4 - X^3 + X^2 + \quad + 1 & \\ - & -X^4 - X^3 - X^2 & \\ \hline & 2X^2 + \quad + 1 & \\ - & 2X^2 + 2X + 2 & \\ \hline & -2X - 1 & \end{array}$$

On en déduit l'égalité $X^5 + X^2 + 1 = (X^2 + X + 1)(X^3 - X^2 + 2) - 2X - 1$. Le quotient de la division euclidienne de $X^5 + X^2 + 1$ par $X^2 + X + 1$ est donc égal à $X^3 - X^2 + 2$ et le reste est $-2X - 1$.

## 3. Plus grand commun diviseur

Si $P$ est un polynôme non nul, tous les diviseurs de $P$ ont un degré plus petit ou égal à celui de $P$. Il n'y a donc qu'un nombre fini de degrés possibles pour les diviseurs de $P$.

**Proposition.** *Si $A$ et $B$ sont des polynômes non tous deux nuls, alors il existe un unique polynôme unitaire de plus grand degré qui divise $A$ et $B$. Ce polynôme s'appelle le* plus grand commun diviseur *de $A$ et $B$ et se note* $\operatorname{pgcd}(A, B)$.

**Démonstration.** Soit $D$ un polynôme de plus grand degré qui divise $A$ et $B$. Si $d$ est le coefficient dominant de $D$, alors le polynôme $(1/d)D$ est un polynôme unitaire de plus grand degré qui divise $A$ et $B$.

Montrons l'unicité. Pour tout entier $n \in \mathbf{N}$, notons $\mathscr{P}_n$ la propriété :

> pour tout polynôme $A$, pour tout polynôme $B$ non nul de degré inférieur ou égal à $n$, il existe un unique polynôme unitaire de plus grand degré qui divise $A$ et $B$.

La propriété $\mathscr{P}_0$ est vraie, car 1 est le seul polynôme unitaire de degré 0.
Soit $n$ un entier tel que $\mathscr{P}_n$ est vraie. Soient $A$ un polynôme et $B$ un polynôme non nul de degré inférieur ou égal à $n+1$. Soient $Q$ et $R$ le quotient et le reste de la division euclidienne de $A$ par $B$. On a $A = BQ + R$ et $R = 0$ ou bien $\deg R < n+1$.
Supposons $R = 0$. Alors $B$ divise $A$ et les diviseurs communs à $A$ et $B$ sont les diviseurs de $B$. Si $Q$ est un diviseur de $B$ de plus grand degré, on a $\deg Q = \deg B$ et il existe un polynôme $S$ tel que $B = QS$. Puisqu'on a $\deg B = \deg Q + \deg S$, il vient $\deg S = 0$, donc $S$ est constant. Si de plus $Q$ est unitaire, alors $Q$ est le quotient de $B$ par son coefficient dominant.
Supposons $R \neq 0$. D'après une remarque du paragraphe précédent, les diviseurs communs à $A$ et $B$ sont les diviseurs communs à $B$ et $R$. Puisqu'on a $\deg R \leqslant n$, il existe un unique polynôme unitaire de plus grand degré qui divise $B$ et $R$, car $\mathscr{P}_n$ est vraie. Il existe donc un unique polynôme unitaire de plus grand degré qui divise $A$ et $B$.
Nous avons ainsi montré que la propriété $\mathscr{P}_{n+1}$ est vraie. D'après le principe de récurrence, la propriété $\mathscr{P}_n$ est vraie quel que soit $n \in \mathbf{N}$. ∎

### Exemples

- Si $P$ est un polynôme unitaire, alors on a $\operatorname{pgcd}(P, 0) = P$. En effet, si $Q$ est un diviseur unitaire de $P$, alors on a $\deg Q \leqslant \deg P$ ; le polynôme $P$ est donc un polynôme unitaire de plus grand degré qui divise $P$ et 0 ; par unicité du pgcd, on en déduit que $P$ est le pgcd de $P$ et 0.
- Pour tout polynôme $P$, on a $\operatorname{pgcd}(P, 1) = 1$.
- Si $P$ est un polynôme non nul et si $Q$ est un diviseur unitaire de $P$, alors $\operatorname{pgcd}(P, Q) = Q$.
- On a $\operatorname{pgcd}(X^{12} - 1, X^8 - 1) = X^4 - 1$.

### Remarque

Si $P$ et $Q$ sont des polynômes non tous deux nuls et si $a$ est un élément non nul de $\mathbf{K}$, il vient $\operatorname{pgcd}(aP, Q) = \operatorname{pgcd}(P, Q)$. En particulier, si $P$ est un polynôme non nul, on a $\operatorname{pgcd}(P, 0) = (1/a)P$, où $a$ est le coefficient dominant de $P$.

**Proposition.** *Soient $A$ et $B$ des polynômes non nuls. Si $R$ est le reste de la division euclidienne de $A$ par $B$, alors $\operatorname{pgcd}(A, B) = \operatorname{pgcd}(B, R)$.*



Comme en arithmétique (page 192), nous pouvons, grâce à cette proposition, présenter un algorithme de calcul du plus grand commun diviseur.

## L'algorithme d'Euclide

Soient $A$ et $B$ des polynômes non nuls tels que $\deg A \geqslant \deg B$. Posons $B = R_0$ et notons $R_1$ le reste de la division euclidienne de $A$ par $B$.
Si $R_1 \neq 0$, notons $R_2$ le reste de la division euclidienne de $R_0$ par $R_1$, et ainsi de suite : tant que $R_{n-1} \neq 0$, notons $R_n$ le reste de la division euclidienne de $R_{n-2}$ par $R_{n-1}$. La suite des degrés des polynômes $R_n$ est strictement décroissante, donc il existe un entier positif $N$ tel que le reste de la division euclidienne de $R_{N-1}$ par $R_N$ est nul. D'après la proposition ci-dessus, on a

$$\operatorname{pgcd}(A, B) = \operatorname{pgcd}(R_0, R_1) = \cdots = \operatorname{pgcd}(R_{N-1}, R_N) = \operatorname{pgcd}(R_N, 0).$$

D'après le premier exemple traité, on en déduit l'existence et le calcul du plus grand commun diviseur : il vient $\operatorname{pgcd}(A, B) = (1/a)R_N$, où $a$ est le coefficient dominant du polynôme $R_N$.

> Puisqu'on a $\operatorname{pgcd}(\lambda P, Q) = \operatorname{pgcd}(P, Q)$ pour tout $\lambda \in \mathbf{K}$, $\lambda \neq 0$, on peut dans la pratique remplacer l'un des restes $R_n$ obtenus par $\lambda R_n$, où $\lambda$ est un élément non nul de $\mathbf{K}$.

**Exemple.** Pratiquons l'algorithme d'Euclide pour calculer le plus grand commun diviseur de $X^4 + 4X^3 + X^2 - 16$ et $X^3 + 3X^2 - 3X + 4$. Nous avons

$$X^4 + 4X^3 + X^2 - 16 = (X^3 + 3X^2 - 3X + 4)(X + 1) + X^2 - X - 20$$
$$X^3 + 3X^2 - 3X + 4 = (X^2 - X - 20)(X + 4) + 21(X + 4)$$
$$X^2 - X - 20 = (X + 4)(X - 5)$$

et le plus grand commun diviseur de $X^4 + 4X^3 + X^2 - 16$ et $X^3 + 3X^2 - 3X + 4$ est ainsi égal à $X + 4$.

### Définition

Soient $A$ et $B$ des polynômes non tous deux nuls. On dit que $A$ et $B$ sont *premiers entre eux* si $\operatorname{pgcd}(A, B) = 1$.

**Lemme.** *Soient $A$ et $B$ des polynômes non nuls. Les quotients de $A$ et $B$ par leur plus grand commun diviseur sont des polynômes premiers entre eux.*

**Démonstration.** Posons $D = \operatorname{pgcd}(A, B)$ et $D_1 = \operatorname{pgcd}(A_1, B_1)$, où $A_1$ et $B_1$ sont les quotients respectifs de $A$ et $B$ par $D$. Les polynômes $D$ et $D_1$ sont unitaires, donc le polynôme $DD_1$ est unitaire. Puisque $D_1$ divise $A_1$, $DD_1$ divise $DA_1 = A$. De même, $DD_1$ divise $B$. Le polynôme $DD_1$ est un diviseur commun à $A$ et $B$, donc on a $\deg(DD_1) \leqslant \deg D$, par définition du plus grand commun diviseur. Or on a $\deg(DD_1) = \deg D + \deg D_1$, par suite $\deg D_1 = 0$, c'est-à-dire $D_1$ est un polynôme constant. Le polynôme $D_1$ étant unitaire, il s'ensuit $D_1 = 1$. ■

## 4. Le théorème de Bézout

**Théorème de Bézout.** *Soient $A$ et $B$ des polynômes non nuls. Si $D = \operatorname{pgcd}(A, B)$, alors il existe des polynômes $U$ et $V$ tels que $D = AU + BV$.*

### Exemple de recherche d'une relation de Bézout

Considérons les polynômes $A = X^4 + 4X^3 + X^2 - 16$ et $B = X^3 + 3X^2 - 3X + 4$ dont nous avons calculé le plus grand commun diviseur dans l'exemple précédent. En remontant les égalités de l'algorithme d'Euclide, on obtient

$$\begin{aligned} 21(X+4) &= B - (X^2 - X - 20)(X+4) \\ &= B - \big(A - (X+1)B\big)(X+4) \\ &= (X^2 + 5X + 5)B - (X+4)A \end{aligned}$$

Par conséquent, nous avons la relation de Bézout

$$(X^4 + 4X^3 + X^2 - 16)U + (X^3 + 3X^2 - 3X + 4)V = X + 4$$

où $U$ et $V$ sont les polynômes $U = -(1/21)(X+4)$ et $V = (1/21)(X^2 + 5X + 5)$.

**Théorème.** *Si $A$ et $B$ sont des polynômes non nuls, alors $A$ et $B$ sont premiers entre eux si et seulement s'il existe des polynômes $U$ et $V$ tels que $AU + BV = 1$.*

**Démonstration.** Si $A$ et $B$ sont premiers entre eux, le théorème de Bézout affirme l'existence de $U$ et $V$. Réciproquement, supposons qu'il existe $U$ et $V$ tels que $AU + BV = 1$. Si $D$ est un diviseur de $A$ et $B$, alors $D$ divise $AU$ et $BV$ donc $D$ divise $AU + BV$, par suite $D$ est un polynôme constant non nul. En particulier $\operatorname{pgcd}(A, B)$ est un polynôme constant non nul. Puisque $\operatorname{pgcd}(A, B)$ est un polynôme unitaire, il vient $\operatorname{pgcd}(A, B) = 1$. ■

Comme en arithmétique (pages 193 à 198), le théorème de Bézout permet de caractériser le plus grand commun diviseur parmi tous les diviseurs communs et permet de démontrer le théorème de Gauss.



**Proposition.** *Soient $A$ et $B$ des polynômes non nuls.*
- *Tout diviseur de $A$ et $B$ divise $\operatorname{pgcd}(A, B)$.*
- *Pour tout polynôme $P$ unitaire, on a $\operatorname{pgcd}(PA, PB) = P\operatorname{pgcd}(A, B)$.*

**Démonstration.** La première propriété se démontre comme en arithmétique (page 195). Démontrons la seconde. Soit $P$ un polynôme unitaire. Posons $D = \operatorname{pgcd}(A, B)$. Puisque $DP$ est un diviseur commun de $AP$ et $BP$, $DP$ divise $\operatorname{pgcd}(AP, BP)$. Or $P$ divise $DP$, donc $P$ divise $\operatorname{pgcd}(AP, BP)$. Notons $Q$ le polynôme tel que $\operatorname{pgcd}(AP, BP) = QP$. Le coefficient dominant de $QP$ étant le produit des coefficients dominants de $Q$ et de $P$, on en déduit que le polynôme $Q$ est unitaire. D'autre part, le polynôme $QP$ divise $AP$ et $BP$, par suite $Q$ divise $A$ et $B$ et donc $Q$ divise $D$. Puisque $DP$ divise $QP$ et puisque $P$ n'est pas nul, $D$ divise $Q$. Il s'ensuit que $D$ divise $Q$ et $Q$ divise $D$. Il existe donc $a \in \mathbf{K}$, $a \neq 0$ tel que $D = aQ$. Les polynômes $D$ et $Q$ étant unitaires, il vient $a = 1$ et $D = Q$, d'où $\operatorname{pgcd}(AP, BP) = DP$. ■

**Théorème de Gauss.** *Soient $A, B, C$ des polynômes non nuls. Si $A$ divise $BC$ et si $A$ et $B$ sont premiers entre eux, alors $A$ divise $C$.*

**Corollaire.** *Si $A$ et $B$ sont des polynômes non constants et premiers entre eux, alors il existe des polynômes non nuls $U$ et $V$ uniques tels que $AU + BV = 1$, $\deg U < \deg B$ et $\deg V < \deg A$.*

**Démonstration.** D'après le théorème de Bézout, il existe des polynômes $S$ et $T$ tels que $AS + BT = 1$. Notons $Q$ le quotient et $U$ le reste de la division euclidienne de $S$ par $B$. Il vient $1 = AS + BT = A(BQ + U) + BT = B(AQ + T) + AU$. On a forcément $U \neq 0$, car sinon on aurait $1 = B(AQ + T)$, ce qui est impossible, puisque le polynôme $B$ n'est pas constant. Posons alors $V = T + AQ$. On a $AU + BV = 1$. Puisque $A$ n'est pas constant et que $U$ est non nul, $AU$ n'est pas constant, donc $BV = 1 - AU$ est non nul, ce qui implique $V \neq 0$. Il vient alors $\deg(AU) = \deg(BV)$, c'est-à-dire $\deg B + \deg V = \deg A + \deg U$. Enfin, puisque $U$ est le reste de la division euclidienne de $S$ par $B$, on a $\deg U < \deg B$ et par suite $\deg V < \deg A$, d'où l'existence de $U$ et $V$. Démontrons l'unicité de $U$ et $V$. Soient $U_1$ et $V_1$ des polynômes vérifiant l'énoncé du corollaire, ainsi que $U_2$ et $V_2$. Il vient $A(U_1 - U_2) = B(V_2 - V_1)$ et il s'ensuit que $A$ divise $B(V_2 - V_1)$. Puisque $A$ et $B$ sont premiers entre eux, $A$ divise $V_2 - V_1$, d'après le théorème de Gauss. D'autre part, on a $\deg V_2 < \deg A$ et $\deg V_1 < \deg A$ donc $V_2 - V_1 = 0$ ou bien $V_2 - V_1 \neq 0$ et $\deg(V_2 - V_1) < \deg A$. Puisque tout multiple non nul de $A$ est de degré supérieur ou égal à celui de $A$, on en déduit $V_2 - V_1 = 0$ et $U_1 - U_2 = 0$, c'est-à-dire $V_1 = V_2$ et $U_1 = U_2$, d'où l'unicité des polynômes $U$ et $V$. ■

Grâce au théorème de Gauss, nous sommes en mesure de trouver tous les polynômes $P$ et $Q$ solutions d'une équation du type $AP + BQ = C$.

### Exercice

**a)** Existe-il $P, Q \in \mathbf{Q}[X]$ tels que $(X^6-1)P+(X^{10}-1)Q = X^2+1$ ? Si oui, trouver tous les polynômes $P, Q \in \mathbf{Q}[X]$ tels que $(X^6-1)P+(X^{10}-1)Q = X^2+1$.

**b)** Existe-il $P, Q \in \mathbf{Q}[X]$ tels que $(X^6-1)P+(X^{10}-1)Q = X^3+X^2-X-1$ ? Si oui, trouver tous les polynômes $P, Q \in \mathbf{Q}[X]$ tels que $(X^6-1)P+(X^{10}-1)Q = X^3+X^2-X-1$.

**Réponse.** Calculons le plus grand commun diviseur de $X^6-1$ et $X^{10}-1$. Pratiquons pour cela l'algorithme d'Euclide. Nous avons

$$X^{10}-1 = (X^6-1)X^4 + X^4 - 1$$
$$X^6-1 = (X^4-1)X^2 + X^2 - 1$$
$$X^4-1 = (X^2-1)(X^2+1)$$

et le plus grand commun diviseur de $X^6-1$ et $X^{10}-1$ est ainsi égal à $X^2-1$. En particulier, $X^2-1$ est un diviseur de $X^6-1$ et $X^{10}-1$. Précisément, nous avons

$$\begin{cases} X^6-1 = (X^2-1)(X^4+X^2+1) \\ X^{10}-1 = (X^2-1)(X^8+X^6+X^4+X^2+1). \end{cases}$$

Il s'ensuit que pour tous $P, Q \in \mathbf{Q}[X]$, $X^2-1$ divise $(X^6-1)P+(X^{10}-1)Q$.

**a)** Puisque le reste de la division euclidienne de $X^2+1$ par $X^2-1$ est égal à 2, le polynôme $X^2+1$ n'est pas multiple de $X^2-1$. Il n'existe donc pas de polynômes $P$ et $Q$ tels que $(X^6-1)P+(X^{10}-1)Q = X^2+1$.

**b)** D'après le théorème de Bézout, il existe des polynômes $U$ et $V$ à coefficients dans $\mathbf{Q}$ tels que $(X^6-1)U+(X^{10}-1)V = X^2-1$. Puisque $X^3+X^2-X-1 = (X^2-1)(X+1)$, il existe des polynômes $P$ et $Q$ à coefficients dans $\mathbf{Q}$ tels que $(X^6-1)P+(X^{10}-1)Q = X^3+X^2-X-1$, par exemple les polynômes $P=(X+1)U$ et $Q=(X+1)V$.

*Recherche d'une solution particulière.* En utilisant l'algorithme d'Euclide, nous avons les égalités

$$\begin{aligned} X^2-1 &= X^6-1-(X^4-1)X^2 \\ &= X^6-1-((X^{10}-1)-(X^6-1)X^4)X^2 \\ &= (X^6-1)(X^6+1)-(X^{10}-1)X^2. \end{aligned}$$

Puisqu'on a $(X^6+1)(X+1) = X^7+X^6+X+1$ et $X^2(X+1) = X^3+X^2$, on en déduit la relation

$$(X^6-1)(X^7+X^6+X+1)-(X^{10}-1)(X^3+X^2) = X^3+X^2-X-1.$$

*Recherche de toutes les solutions.* Posons $P_0 = X^7+X^6+X+1$ et $Q_0 = -X^3-X^2$. Soient $P$ et $Q$ des polynômes à coefficients dans $\mathbf{Q}$ tels que

$$(X^6-1)P+(X^{10}-1)Q = X^3+X^2-X-1.$$

D'après ce qui précède, il vient $(X^6-1)(P-P_0) = (X^{10}-1)(Q_0-Q)$, ou encore

$$(X^2-1)(X^4+X^2+1)(P-P_0) = (X^2-1)(X^8+X^6+X^4+X^2+1)(Q_0-Q).$$

Il s'ensuit l'égalité $(X^4+X^2+1)(P-P_0) = (X^8+X^6+X^4+X^2+1)(Q_0-Q)$. Puisque $X^4+X^2+1$ et $X^8+X^6+X^4+X^2+1$ sont les quotients respectifs de $X^6-1$ et $X^{10}-1$ par leur plus grand commun diviseur, ces deux polynômes sont premiers entre eux.





D'après le théorème de Gauss, on en déduit que $X^8+X^6+X^4+X^2+1$ divise $P-P_0$. Il existe donc $S \in \mathbf{Q}[X]$ tel que $P-P_0 = (X^8+X^6+X^4+X^2+1)S$. En reportant cette égalité dans $(X^4+X^2+1)(P-P_0) = (X^8+X^6+X^4+X^2+1)(Q_0-Q)$, nous obtenons $Q_0-Q = (X^4+X^2+1)S$. Les polynômes $P$ et $Q$ tels que $(X^6-1)P+(X^{10}-1)Q = X^3+X^2-X-1$ sont finalement les polynômes $P$ et $Q$ de la forme

$$P = P_0+(X^8+X^6+X^4+X^2+1)S \quad \text{et} \quad Q = Q_0-(X^4+X^2+1)S,$$

où $S \in \mathbf{Q}[X]$. En effet, il est clair que de tels polynômes vérifient la relation demandée.

## 5. Racine d'un polynôme

Soient $P$ un polynôme et $a$ un élément de $\mathbf{K}$. Si $P$ est le polynôme constant égal à $\lambda$, on pose $P(a) = \lambda$. S'il existe un entier positif $n$ tel que $P = a_nX^n+\cdots+a_1X+a_0$, où $a_n \neq 0$, on pose $P(a) = a_na^n+\cdots+a_1a+a_0$.

La fonction de $\mathbf{K}$ dans $\mathbf{K}$ qui à tout élément $x \in \mathbf{K}$ associe $P(x)$ s'appelle la *fonction polynôme* associée à $P$.

La démonstration du lemme suivant est immédiate.

**Lemme.** *Soient $P, Q$ des polynômes et $\lambda, a$ des éléments de $\mathbf{K}$. Alors on a*

$$(\lambda P)(a) = \lambda P(a), \quad (P+Q)(a) = P(a)+Q(a) \quad \text{et} \quad (PQ)(a) = P(a)Q(a).$$

**Définition**

Soient $P$ un polynôme et $a$ un élément de $\mathbf{K}$. On dit que $a$ est *racine* de $P$ si $P(a)=0$.

**Proposition.** *Soient $P$ un polynôme et $a$ un élément de $\mathbf{K}$. Le reste de la division euclidienne de $P$ par $X-a$ est égal à $P(a)$.*

**Démonstration.** Posons $S = X-a$ et notons $Q$ le quotient et $R$ le reste de la division euclidienne de $P$ par $S$. Puisque $S$ est de degré 1, ou bien $R$ est nul, ou bien $\deg R = 0$. En tous cas, $R$ est un polynôme constant. D'autre part, on a $P = SQ+R$, donc $P(a) = S(a)Q(a)+R(a)$, d'après le lemme ci-dessus. Or on a $S(a) = a-a = 0$, par suite $P(a) = R(a)$. Le polynôme $R$ étant constant, il s'ensuit $R = P(a)$. ∎

**Corollaire.** *Soient $P$ un polynôme et $a$ un élément de $\mathbf{K}$. Le nombre $a$ est racine de $P$ si et seulement si le polynôme $X-a$ divise $P$.*

**Proposition.** *Soit $n$ un entier positif. Si $P$ est un polynôme de degré $n$, alors $P$ a au plus $n$ racines dans $\mathbf{K}$.*

**Démonstration.** On démontre ce résultat par récurrence sur $n$. Si $n = 1$, il existe $a, b \in \mathbf{K}$ tels que $P = aX + b$ et $a \neq 0$. Le polynôme $P$ a donc exactement une racine dans $\mathbf{K}$ : $-b/a$. Si $n \geqslant 2$, alors ou bien $P$ n'a pas de racine dans $\mathbf{K}$ (et dans ce cas il en a au plus $n$), ou bien $P$ a au moins une racine dans $\mathbf{K}$. Supposons que l'élément $a \in \mathbf{K}$ est racine de $P$. D'après le corollaire précédent, il existe un polynôme $Q \in \mathbf{K}[X]$ tel que $P = (X - a)Q$. Le polynôme $Q$ est de degré $n - 1$, donc par hypothèse de récurrence, $Q$ a au plus $n - 1$ racines. Il s'ensuit que $P$ a au plus $n$ racines. ■

**Exemples**

- Le polynôme $X^2 - 2$ n'a pas de racine appartenant à $\mathbb{Q}$, mais a deux racines réelles : $\sqrt{2}$ et $-\sqrt{2}$.
- Le polynôme $X^4 + 1$ n'a pas de racine réelle, mais a quatre racines complexes : $\frac{1+i}{\sqrt{2}}$, $\frac{1-i}{\sqrt{2}}$, $\frac{-1-i}{\sqrt{2}}$ et $\frac{-1+i}{\sqrt{2}}$.

**Proposition.** *Soient $a, b, c \in \mathbf{K}$. On suppose $a \neq 0$ et l'on pose $P = aX^2 + bX + c$ et $\Delta = b^2 - 4ac$.*

- *Si $\Delta$ n'est pas le carré d'un élément de $\mathbf{K}$, alors $P$ n'a pas de racine dans $\mathbf{K}$.*
- *Si $\Delta = 0$, alors $P$ a une racine dans $\mathbf{K}$ : $-b/2a$.*
- *Si $\Delta \neq 0$ et s'il existe $\delta \in \mathbf{K}$ tel que $\Delta = \delta^2$, alors $P$ a deux racines dans $\mathbf{K}$ : $(-b+\delta)/2a$ et $(-b-\delta)/2a$.*

**Démonstration.** Écrivons $X^2 + (b/a)X$ comme le début d'un carré : $X^2 + (b/a)X = (X + b/2a)^2 - b^2/4a^2$. On en déduit l'égalité $P = a\big((X + b/2a)^2 - \Delta/4a^2\big)$. S'il existe $\alpha \in \mathbf{K}$ tel que $P(\alpha) = 0$, on a donc $\Delta = 4a^2(\alpha + b/2a)^2 = (2a\alpha + b)^2$. Il s'ensuit que si $P$ a une racine dans $\mathbf{K}$, alors il existe $\delta \in \mathbf{K}$ tel que $\delta^2 = \Delta$.

Réciproquement, supposons qu'il existe $\delta \in \mathbf{K}$ tel que $\delta^2 = \Delta$. Si $\Delta = 0$, alors $\delta = 0$, $P = a(X + b/2a)^2$ et $P$ n'a qu'une seule racine dans $\mathbf{K}$ : $-b/2a$. Si $\Delta \neq 0$, alors $\delta \neq 0$ et l'on a $P = a\big(X + (b+\delta)/2a\big)\big(X + (b-\delta)/2a\big)$. Le polynôme $P$ a donc deux racines dans $\mathbf{K}$ : $-(b+\delta)/2a$ et $-(b-\delta)/2a$. ■

**Définition**

Si $P$ est un polynôme de degré 2, le nombre $\Delta$ de la proposition ci-dessus s'appelle le *discriminant* de $P$.

**Exemples**

- Puisque tout nombre complexe a une racine carrée dans $\mathbb{C}$ (voir chapitre 3), tout polynôme de degré 2 de $\mathbb{C}[X]$ a au moins une racine dans $\mathbb{C}$.





- Puisqu'un nombre réel est le carré d'un nombre réel si et seulement s'il est positif ou nul, on en déduit qu'un polynôme de degré 2 de $\mathbb{R}[X]$ a une racine réelle si et seulement si son discriminant est positif ou nul.
- Il existe des polynômes de degré 2 de $\mathbb{Q}[X]$ qui ont une racine réelle mais qui n'ont pas de racine rationnelle. Par exemple $X^2 - p$, où $p$ est un nombre premier, et plus généralement $X^2 - n$, où $n$ est un entier supérieur ou égal à 2, sans facteur carré (voir page 200).

**Remarque**

Soit $P$ un polynôme unitaire et de degré 2. Si $\alpha$ et $\beta$ sont les racines complexes de $P$ et si $P = X^2 + pX + q$, alors il vient $\alpha + \beta = -p$ et $\alpha\beta = q$. En effet, on a

$$P = (X - \alpha)(X - \beta) = X^2 - (\alpha + \beta)X + \alpha\beta.$$

**Définition**

Soient $P$ un polynôme non constant et $a$ un élément de $\mathbf{K}$. On suppose que $a$ est racine de $P$. Le plus grand entier positif $r$ tel que $(X - a)^r$ divise $P$ s'appelle *l'ordre de multiplicité* de la racine $a$ dans $P$. Si $r = 1$, on dit que $a$ est racine *simple* de $P$ et si $r \geqslant 2$, on dit que $a$ est racine *multiple* de $P$.

**Proposition.** *Soient $P$ un polynôme non constant et $a$ un élément de $\mathbf{K}$. Le nombre $a$ est racine multiple de $P$ si et seulement si l'on a $P(a) = P'(a) = 0$.*

**Démonstration.** Supposons que $a$ est racine de $P$. D'après le corollaire page 231, il existe un polynôme $Q$ tel que $P = (X - a)Q$. Le polynôme $(X - a)^2$ divise donc $P$ si et seulement si $X - a$ divise $Q$, c'est-à-dire si et seulement si $Q(a) = 0$. Or on a $P' = (X - a)Q' + Q$, par suite $Q(a) = P'(a)$, d'où le résultat. ■

Rappelons la propriété suivante qui est une conséquence du théorème des valeurs intermédiaires (voir le tome d'analyse) : tout polynôme à coefficients réels et de degré impair a une racine réelle.

Voici un énoncé beaucoup plus général concernant les racines de polynômes.

**Théorème de d'Alembert-Gauss.** *Tout polynôme non constant de $\mathbb{C}[X]$ a une racine dans $\mathbb{C}$.*

Ce théorème très important est admis. Sa démonstration utilise des résultats d'analyse, par exemple celui que nous venons de rappeler.

Le théorème affirme notamment que si $P$ est un polynôme non constant à coefficients réels, il existe au moins un nombre complexe $a$ tel que $P(a) = 0$ ; il résulte de la proposition suivante qu'on a alors aussi $P(\bar{a}) = 0$.

**Proposition.** *Soit $P \in \mathbb{R}[X]$. Pour tout nombre complexe $z$, on a $P(\bar{z}) = \overline{P(z)}$.*

**Démonstration.** Posons $P = a_n X^n + \cdots + a_1 X + a_0$ où $a_0, a_1, \ldots, a_n$ sont des nombres réels. On a $P(z) = a_n z^n + \cdots + a_1 z + a_0$ et d'après les règles de conjugaison (voir chapitre 3), il vient

$$\begin{aligned} \overline{P(z)} &= \overline{a_n z^n + \cdots + a_1 z + a_0} \\ &= \overline{a_n z^n} + \cdots + \overline{a_1 z} + \overline{a_0} \quad \text{(conjugué d'une somme)} \\ &= \overline{a_n}\ \bar{z}^n + \cdots + \overline{a_1}\ \bar{z} + \overline{a_0} \quad \text{(conjugué d'un produit)} \\ &= a_n \bar{z}^n + \cdots + a_1 \bar{z} + a_0 \quad \text{(car les nombres } a_i \text{ sont réels)} \\ &= P(\bar{z}). \end{aligned}$$

■

**Proposition.** *Si $P$ et $Q$ sont des polynômes non constants, alors les racines communes à $P$ et $Q$ dans $\mathbb{C}$ sont les racines complexes de $\mathrm{pgcd}(P, Q)$.*

**Démonstration.** Posons $D = \mathrm{pgcd}(P, Q)$. Si $a$ est un nombre complexe tel que $D(a)=0$, alors on a $P(a)=0$ et $Q(a)=0$, car les polynômes $P$ et $Q$ sont multiples de $D$. Réciproquement, supposons qu'il existe $a \in \mathbb{C}$ tel que $P(a) = Q(a) = 0$. Le polynôme $X - a$ divise $P$ et $Q$, donc divise $D$ ; le nombre $a$ est ainsi racine de $D$. ■

Appliquons la proposition en choisissant pour $P$ un polynôme de degré supérieur ou égal à 2 et en posant $Q = P'$. On en déduit que les racines communes à $P$ et $P'$ sont les racines complexes de $\mathrm{pgcd}(P, P')$, c'est-à-dire les racines multiples de $P$. Puisqu'un polynôme possède une racine complexe si et seulement s'il est non constant, il s'ensuit que $P$ a une racine multiple si et seulement si $\mathrm{pgcd}(P, P')$ est non constant. Énonçons ces résultats.

**Corollaire.** *Soit $P$ un polynôme de degré supérieur ou égal à 2. Le polynôme $P$ a une racine multiple dans $\mathbb{C}$ si et seulement si $\mathrm{pgcd}(P, P')$ est un polynôme non constant. De plus, les racines multiples de $P$ dans $\mathbb{C}$ sont les racines complexes de $\mathrm{pgcd}(P, P')$.*



**Exercice 1.** Les polynômes $X^5 + 3X^3 + 2X^2 - 4X + 8$ et $X^4 + X^3 + 6X^2 + 4X + 8$ ont-ils une racine commune dans $\mathbb{C}$ ? En déduire toutes les racines complexes de $X^4 + X^3 + 6X^2 + 4X + 8$.

**Réponse.** Pratiquons l'algorithme d'Euclide pour calculer le plus grand commun diviseur de $X^5 + 3X^3 + 2X^2 - 4X + 8$ et $X^4 + X^3 + 6X^2 + 4X + 8$. Il vient

$$\begin{aligned} X^5 + 3X^3 + 2X^2 - 4X + 8 &= (X - 1)(X^4 + X^3 + 6X^2 + 4X + 8) \\ &\quad - 2(X^3 - 2X^2 + 4X - 8) \\ X^4 + X^3 + 6X^2 + 4X + 8 &= (X^3 - 2X^2 + 4X - 8)(X + 3) + 8(X^2 + 4) \\ X^3 - 2X^2 + 4X - 8 &= (X^2 + 4)(X - 2) \end{aligned}$$

et le plus grand commun diviseur de $X^5+3X^3+2X^2-4X+8$ et $X^4+X^3+6X^2+4X+8$ est ainsi égal à $X^2 + 4$.

Les racines complexes communes à ces deux polynômes sont donc les racines complexes de $X^2 + 4$, c'est-à-dire $2i$ et $-2i$. Puisque $X^2 + 4$ est le plus grand commun diviseur des polynômes considérés, $X^2 + 4$ divise $X^4 + X^3 + 6X^2 + 4X + 8$. Précisément on a

$$X^4 + X^3 + 6X^2 + 4X + 8 = (X^2 + 4)(X^2 + X + 2).$$

Il reste à calculer les racines complexes de $X^2 + X + 2$. Le discriminant de $X^2 + X + 2$ est égal à $-7$ et les racines sont $(-1 + i\sqrt{7})/2$ et $(-1 - i\sqrt{7})/2$. Les racines complexes de $X^4 + X^3 + 6X^2 + 4X + 8$ sont donc $2i$, $-2i$, $(-1 + i\sqrt{7})/2$ et $(-1 - i\sqrt{7})/2$. Ce sont des racines simples.

**Exercice 2.** Le polynôme $X^4 + 4X^3 + 10X^2 + 12X + 9$ a-t-il une racine multiple dans $\mathbb{C}$ ? En déduire toutes les racines complexes de $X^4 + 4X^3 + 10X^2 + 12X + 9$.

**Réponse.** Posons $P = X^4 + 4X^3 + 10X^2 + 12X + 9$. Il vient $P' = 4(X^3 + 3X^2 + 5X + 3)$. Pratiquons l'algorithme d'Euclide pour calculer le plus grand commun diviseur de $P$ et $P'$. Nous avons

$$\begin{aligned} X^4 + 4X^3 + 10X^2 + 12X + 9 &= \\ (X^3 + 3X^2 + 5X + 3)&(X + 1) + 2(X^2 + 2X + 3) \\ X^3 + 3X^2 + 5X + 3 &= (X^2 + 2X + 3)(X + 1) \end{aligned}$$

et le plus grand commun diviseur de $P$ et $P'$ est ainsi égal à $X^2 + 2X + 3$.

Les racines multiples de $P$ dans $\mathbb{C}$ sont donc les racines complexes de $X^2 + 2X + 3$, c'est-à-dire $-1 + i\sqrt{2}$ et $-1 - i\sqrt{2}$. Puisque le polynôme $X^2 + 2X + 3$ est le plus grand commun diviseur de $P$ et $P'$, $X^2 + 2X + 3$ divise $P$. Précisément on a $P = (X^2 + 2X + 3)^2$. Les racines complexes de $P$ sont donc $-1 + i\sqrt{2}$ et $-1 - i\sqrt{2}$, et chacune de ces racines est d'ordre de multiplicité 2.

**Exercice 3**

a) Trouver un polynôme $P$ à coefficients rationnels et de degré 4, ayant pour racine le nombre $\sqrt{2}+\sqrt{3}$.

b) Quelles sont les racines de $P$ ?

**Réponse**

a) Posons $x=\sqrt{2}+\sqrt{3}$. On a $x^2=(\sqrt{2}+\sqrt{3})^2=2+2\sqrt{2}\sqrt{3}+3=5+2\sqrt{2}\sqrt{3}$, d'où

$$(x^2-5)^2=4\times 2\times 3=24\,.$$

Le polynôme $P=(X^2-5)^2-24$ a donc pour racine le nombre $x$. De plus, $P$ est de degré 4 et ses coefficients sont des nombres rationnels.

b) Dans le calcul précédent, les seules propriétés des nombres $\sqrt{2}$ et $\sqrt{3}$ que nous avons utilisées sont les relations $(\sqrt{2})^2=2$ et $(\sqrt{3})^2=3$. Comme on a aussi $(-\sqrt{2})^2=2$ et $(-\sqrt{3})^2=3$, on en déduit que

$$P(\sqrt{2}+\sqrt{3})=P(\sqrt{2}-\sqrt{3})=P(-\sqrt{2}+\sqrt{3})=P(-\sqrt{2}-\sqrt{3})\,.$$

Les nombres $\sqrt{2}-\sqrt{3}$, $-\sqrt{2}+\sqrt{3}$ et $-\sqrt{2}-\sqrt{3}$ sont donc aussi des racines de $P$. Puisque $P$ est de degré 4, ses racines sont les quatre nombres $\sqrt{2}+\sqrt{3}$, $\sqrt{2}-\sqrt{3}$, $-\sqrt{2}+\sqrt{3}$ et $-\sqrt{2}-\sqrt{3}$.

## 6. Polynôme irréductible

Pour tout polynôme $P\in\mathbf{K}[X]$ et pour tout élément non nul $a\in\mathbf{K}$, on a $P=(1/a)aP$. Il y a des polynômes pour lequel il n'y a pas d'autre factorisation : les polynômes *irréductibles*. La notion correspondante en arithmétique est celle de nombre premier.

**Définition**

Un *polynôme irréductible* est un polynôme $P$ non constant dont les seuls diviseurs sont les polynômes constants et les polynômes de la forme $aP$, où $a$ est un élément non nul de $\mathbf{K}$.

Supposons que $P$ est un polynôme non constant. Dire que $P$ n'est pas irréductible signifie que $P$ possède un diviseur non constant de degré strictement plus petit que celui de $P$. Autrement dit, le polynôme $P$ n'est pas irréductible si et seulement s'il existe des polynômes non constants $Q$ et $R$ tels que $P=QR$.

**Exemples**

- Les polynômes de degré 1 sont des polynômes irréductibles.
- Le polynôme $X^2-2$ n'est pas un polynôme irréductible de $\mathbb{R}[X]$, puisqu'il est divisible par $X-\sqrt{2}$. Par contre, $X^2-2$ est un polynôme irréductible de $\mathbb{Q}[X]$.



**Lemme.** *Soient $Q$ un polynôme non nul et $P$ un polynôme irréductible. Alors ou bien $P$ divise $Q$, ou bien $P$ et $Q$ sont premiers entre eux.*

**Démonstration.** Notons $D$ le plus grand commun diviseur de $P$ et $Q$. En particulier, $D$ est un diviseur unitaire de $P$, par suite $D=1$ ou $D=(1/a)P$, si $a$ est le coefficient dominant de $P$. Dans ce dernier cas, $P$ divise $Q$. ∎

**Lemme d'Euclide.** *Soient $A$ et $B$ des polynômes non nuls et $P$ un polynôme irréductible. Si $P$ divise $AB$, alors $P$ divise $A$ ou $P$ divise $B$.*

Nous avons montré en arithmétique que tout entier positif différent de 1 est produit de nombres premiers. De même nous allons voir que tout polynôme non constant est produit de polynômes irréductibles.

**Théorème.** *Soit $P$ un polynôme non constant et unitaire. Alors il existe un unique entier positif $r$ et des polynômes irréductibles et unitaires $P_1,\ldots,P_r$, uniques à permutation près, tels que $P=P_1\cdots P_r$.*

**Démonstration.** On démontre l'existence d'une telle factorisation par récurrence sur le degré de $P$. Si $P$ est de degré 1, alors $P$ est un polynôme irréductible et unitaire. Si $P$ est de degré supérieur ou égal à 2, notons $P_1$ un diviseur non constant et unitaire de $P$, de plus bas degré. Un diviseur unitaire de $P_1$ est de degré inférieur ou égal à celui de $P_1$ et divise $P$, donc est égal 1 ou à $P_1$. On en déduit que $P_1$ est un polynôme irréductible. Si $\deg P=\deg P_1$, alors $P=P_1$ et c'est fini. Si $\deg P>\deg P_1$, notons $Q$ le quotient de $P$ par $P_1$. Le polynôme $Q$ est non constant, unitaire et de degré strictement inférieur à celui de $P$. On conclut en appliquant l'hypothèse de récurrence au polynôme $Q$.

On démontre l'unicité d'une telle factorisation également par récurrence sur le degré de $P$. Supposons que l'on a $P=P_1\cdots P_r$, où $r$ et les $P_i$ sont comme dans le théorème et aussi $P=Q_1\cdots Q_s$, où $s$ et les $Q_j$ sont comme dans le théorème. D'après le lemme d'Euclide, $P_1$ divise au moins l'un des $Q_j$. Quitte à rénuméroter les $Q_j$, on peut supposer que $P_1$ divise $Q_1$. Puisque $Q_1$ est irréductible et $P_1$ est non constant, il existe $\lambda\in\mathbf{K}$ tel que $P_1=\lambda Q_1$. Enfin, les polynômes $P_1$ et $Q_1$ sont unitaires, par suite $P_1=Q_1$. Si $\deg P=\deg P_1$, alors $P=P_1$ et $s=1$. Si $\deg P>\deg P_1$, on conclut en appliquant l'hypothèse de récurrence au quotient de $P$ par $P_1$. ∎

**Proposition.** *Soit $P$ un polynôme de degré 2 ou 3. Le polynôme $P$ est irréductible si et seulement si $P$ n'a pas de racine dans $\mathbf{K}$.*

**Démonstration.** Si $P$ a une racine dans $\mathbf{K}$, alors $X-a$ divise $P$ et le quotient $Q$ est un polynôme non constant, d'après l'hypothèse sur le degré de $P$. Il s'ensuit que le polynôme $P$ n'est pas irréductible.

Réciproquement, supposons que $P$ n'est pas irréductible. Il existe donc des polynômes non constants $Q$ et $R$ tels que $P = QR$. Il vient $\deg P = \deg Q + \deg R$. Puisque $\deg P$ est égal à 2 ou 3 et puisque $\deg Q$ et $\deg R$ sont supérieurs ou égaux à 1, nécessairement l'un des polynômes $Q$ ou $R$ est de degré 1. Supposons par exemple $Q$ de degré 1. On a donc $Q = aX + b$, où $a \neq 0$. Il vient $Q(-b/a) = 0$. Or on a $P(-b/a) = Q(-b/a)R(-b/a)$, par suite $P(-b/a) = 0$. ∎

**Remarque**
Un polynôme irréductible de $\mathbf{K}[X]$ et de degré au moins égal à 2 n'a pas de racine dans $\mathbf{K}$ : cela résulte de la première partie de la démonstration précédente. Mais attention, la réciproque est fausse : un polynôme de degré supérieur ou égal à 4 peut fort bien ne pas avoir de racine dans $\mathbf{K}$ et ne pas être irréductible dans $\mathbf{K}[X]$. Par exemple, le polynôme $(X^2+1)^2$ de $\mathbb{R}[X]$ n'a pas de racine dans $\mathbb{R}$ et n'est pas non plus irréductible.

Pour terminer, voici la liste des polynômes irréductibles de $\mathbb{C}[X]$ et de $\mathbb{R}[X]$.

**Théorème.** *Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1. Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 dont le discriminant est strictement négatif.*

**Démonstration.** Soit $P$ un polynôme irréductible de $\mathbb{C}[X]$. D'après le théorème de d'Alembert-Gauss, il existe $a \in \mathbb{C}$ tel que $P(a) = 0$. Le polynôme $X - a$ est donc un diviseur de $P$. Puisque $X - a$ est non constant, on en déduit qu'il existe un nombre complexe non nul $\lambda$ tel que $P = \lambda(X - a)$. Le polynôme $P$ est donc de degré 1.

Puisqu'un polynôme de $\mathbb{R}[X]$ de degré 2 dont le discriminant est strictement négatif n'a pas de racine réelle, c'est un polynôme irréductible de $\mathbb{R}[X]$.

Réciproquement, soit $P$ un polynôme irréductible de $\mathbb{R}[X]$ de degré supérieur ou égal à 2. D'après le théorème de d'Alembert-Gauss, $P$ a une racine complexe $a$.

Montrons que l'on a $a \neq \bar{a}$ en raisonnant par l'absurde. Si $a = \bar{a}$, alors le nombre complexe $a$ est réel, donc est une racine réelle de $P$. Il s'ensuit que $X - a$ appartient à $\mathbb{R}[X]$ et divise $P$, ce qui est impossible puisque $P$ est un polynôme irréductible, de degré supérieur ou égal à 2. Ainsi nous avons $a \neq \bar{a}$.

Puisque $a$ est racine de $P$, il existe $Q \in \mathbb{C}[X]$ tel que $P = (X - a)Q$. D'autre part, le polynôme $P$ est à coefficients réels, par suite on a $P(\bar{a}) = \overline{P(a)} = 0$. Il vient $0 = P(\bar{a}) = (\bar{a} - a)Q(\bar{a})$ et donc $Q(\bar{a}) = 0$, puisque $\bar{a} - a \neq 0$. Ainsi $\bar{a}$ est racine de $Q$, ce qui signifie que $X - \bar{a}$ divise $Q$. Finalement le polynôme $S = (X - a)(X - \bar{a})$ divise $P$. Or on a $S = X^2 - (a + \bar{a})X + |a|^2$, par suite $S$ est un polynôme à coefficients réels. Enfin, puisque $S$ est de degré 2 et n'a pas de racine réelle, $S$ est un polynôme irréductible de $\mathbb{R}[X]$. Le polynôme $S$ est non constant et $P$ est un polynôme irréductible de $\mathbb{R}[X]$, par suite il existe $\lambda \in \mathbb{R}$, $\lambda \neq 0$, tel que $P = \lambda S$. Le polynôme $P$ est donc de degré 2. ∎





**Exercice 1**

a) Montrer que $X^3 - 2$ n'a pas de racine dans $\mathbf{Q}$.

b) Le polynôme $X^3 - 2$ est-il un polynôme irréductible de $\mathbf{Q}[X]$ ?

**Réponse**

a) Le polynôme $X^3 - 2$ a une seule racine réelle, $\sqrt[3]{2}$. Il s'agit donc de démontrer que $\sqrt[3]{2}$ n'appartient pas à $\mathbf{Q}$. Raisonnons par l'absurde : supposons qu'il existe des entiers positifs $a$ et $b$ tels que $\sqrt[3]{2} = a/b$. Il vient $a^3 = 2b^3$. Or l'exposant de 2 dans $a^3$ est multiple de 3 et l'exposant de 2 dans $2b^3$ est congru à 1 modulo 3 (voir page 200 pour la définition de l'exposant), donc il y a contradiction.

b) Puisque $X^3 - 2$ est de degré 3 et n'a pas de racine dans $\mathbf{Q}$, on en déduit que $X^3 - 2$ est un polynôme irréductible de $\mathbf{Q}[X]$.

**Exercice 2**

a) Trouver la décomposition de $X^4 + 1$ en produit de polynômes irréductibles et unitaires de $\mathbb{R}[X]$.

b) Quels sont les polynômes unitaires de degré 2 de $\mathbb{R}[X]$ qui divisent $X^4 + 1$ ?

c) Montrer que $X^4 + 1$ est un polynôme irréductible de $\mathbf{Q}[X]$.

**Réponse**

a) Le polynôme $X^4 + 1$ n'a pas de racine réelle, donc $X^4 + 1$ est le produit de deux polynômes unitaires, irréductibles et de degré 2 de $\mathbb{R}[X]$. Remarquons que $X^4 + 1$ est le début d'un carré : $X^4 + 1 = (X^2+1)^2 - 2X^2$. La factorisation de $X^4 + 1$ en produit de polynômes irréductibles et unitaires de $\mathbb{R}[X]$ est donc

$$X^4 + 1 = (X^2 + X\sqrt{2} + 1)(X^2 - X\sqrt{2} + 1).$$

b) Soit $P$ un polynôme unitaire de degré 2 de $\mathbb{R}[X]$ qui divise $X^4 + 1$. Nécessairement, $P$ n'a pas de racine réelle, donc $P$ est irréductible. Le polynôme $P$ est donc l'un des facteurs irréductibles unitaires de $X^4 + 1$, c'est-à-dire d'après (a),

$$P = X^2 + X\sqrt{2} + 1 \quad \text{ou} \quad P = X^2 - X\sqrt{2} + 1.$$

c) Supposons que $P$ est un polynôme unitaire de $\mathbf{Q}[X]$ qui divise $X^4 + 1$. Puisque $P$ n'a pas de racine rationnelle, on a $\deg P \neq 1$. De même, on a $\deg P \neq 3$, sinon le quotient de $X^4 + 1$ par $P$ serait un diviseur de $X^4 + 1$ de degré 1. Si $P$ était de degré 2, alors d'après (b), $P$ serait l'un des polynômes $X^2 + X\sqrt{2} + 1$ ou $X^2 - X\sqrt{2} + 1$, ce qui n'est pas possible puisque $\sqrt{2} \notin \mathbf{Q}$. On en déduit que $P = 1$ ou $P = X^4 + 1$. Nous avons ainsi démontré que $X^4 + 1$ est un polynôme irréductible de $\mathbf{Q}[X]$.

## Exercice 3

**a)** Trouver la décomposition de $X^4 - 2$ en produit de polynômes irréductibles et unitaires de $\mathbb{R}[X]$. Quels sont les polynômes unitaires de degré 2 de $\mathbb{R}[X]$ qui divisent $X^4 - 2$ ?

**b)** Montrer que $X^4 - 2$ n'a pas de racine dans $\mathbb{Q}$.

**c)** Montrer que $X^4 - 2$ est un polynôme irréductible de $\mathbb{Q}[X]$.

**Réponse**

**a)** On a $X^4 - 2 = (X^2 - \sqrt{2})(X^2 + \sqrt{2}) = ((X - \sqrt[4]{2})(X + \sqrt[4]{2})(X^2 + \sqrt{2})$, donc la factorisation de $X^4 - 2$ en produit de polynômes irréductibles et unitaires de $\mathbb{R}[X]$ est

$$X^4 - 2 = (X - \sqrt[4]{2})(X + \sqrt[4]{2})(X^2 + \sqrt{2}).$$

Soit $P$ un polynôme unitaire de degré 2 de $\mathbb{R}[X]$ qui divise $X^4 - 2$. Si $P$ n'a pas de racine réelle, alors $P$ est le facteur irréductible unitaire de degré 2 de $X^4 - 2$, c'est-à-dire $P = X^2 + \sqrt{2}$. Si $P$ a une racine réelle, alors $P$ est produit de deux polynômes de degré 1 à coefficients réels et nécessairement $P = (X - \sqrt[4]{2})(X + \sqrt[4]{2})$.

**b)** Puisque les racines réelles de $X^4 - 2$ sont $\sqrt[4]{2}$ et $-\sqrt[4]{2}$, il s'agit de montrer que $\sqrt[4]{2}$ n'appartient pas à $\mathbb{Q}$. Raisonnons par l'absurde : supposons qu'il existe des entiers positifs $a$ et $b$ tels que $\sqrt[4]{2} = a/b$. Il vient $a^4 = 2b^4$. Or l'exposant de 2 dans $a^4$ est multiple de 4 et l'exposant de 2 dans $2b^4$ est congru à 1 modulo 4, donc il y a contradiction.

**c)** Puisque $X^4 - 2$ n'a pas de racine dans $\mathbb{Q}$, ou bien $X^4 - 2$ est un polynôme irréductible de $\mathbb{Q}[X]$, ou bien $X^4 - 2$ est produit de deux polynômes unitaires, irréductibles et de degré 2 de $\mathbb{Q}[X]$. Mais dans ce dernier cas, les seuls facteurs possibles d'après (a) sont les polynômes $(X^2 + \sqrt{2})$ et $(X^2 - \sqrt{2})$ qui ne sont pas à coefficients rationnels. Par suite $X^4 - 2$ est un polynôme irréductible de $\mathbb{Q}[X]$.

## Exercices

**1.** Soient $P$ et $Q$ des polynômes de $\mathbb{K}[X]$.

**a)** Montrer que si les polynômes $P + Q$ et $P - Q$ sont constants, alors les polynômes $P$ et $Q$ sont constants.

**b)** On suppose le polynôme $P^2 - Q^2$ constant et non nul. Montrer que les polynômes $P$ et $Q$ sont constants.

**2. a)** Montrer que les polynômes $X^4 + 1$ et $X^3 + 1$ sont premiers entre eux.

**b)** Trouver tous les polynômes $U$ et $V$ de $\mathbb{Q}[X]$ tels que $(X^4 + 1)U - (X^3 + 1)V = 2$.

**c)** Trouver tous les polynômes $P \in \mathbb{Q}[X]$ tels que $X^4 + 1$ divise $P$ et $X^3 + 1$ divise $P - 2$.

**3. a)** Calculer le plus grand commun diviseur de $X^{21} + 1$ et $X^{15} + 1$.

**b)** Démontrer qu'il existe des polynômes $U, V \in \mathbb{Q}[X]$ uniques tels que $(X^{21} + 1)U - (X^{15} + 1)V = X^3 + 1$, $\deg U < 12$ et $\deg V < 18$.



**4.** Soient $a$ un nombre complexe non nul et $n, k$ des entiers positifs tels que $n > k$.

**a)** Notons $q$ le quotient et $r$ le reste de la division euclidienne de $n$ par $k$. Montrer que le reste de la division euclidienne de $X^n - a^n$ par $X^k - a^k$ est égal à $a^{kq}(X^r - a^r)$.

**b)** Notons $d$ le plus grand commun diviseur de $n$ et $k$. Montrer que le plus grand commun diviseur de $X^n - a^n$ et $X^k - a^k$ est égal à $X^d - a^d$.

**5. a)** Soit $P$ un polynôme à coefficients réels. Notons $R$ le reste de la division euclidienne de $P$ par $X^2 + 1$. Montrer que $R(i) = P(i)$. En déduire que $X^2 + 1$ divise $P$ si et seulement si $P(i) = 0$.

**b)** Pour quels entiers positifs $n$ le polynôme $X^n + 1$ est-il multiple de $X^2 + 1$ ?

**6. a)** Les polynômes $X^6 + X^4$ et $X^{25} - X + 1$ ont-ils une racine commune dans $\mathbb{C}$ ?

**b)** Montrer que les polynômes $X^6 + X^4$ et $X^{25} - X + 1$ sont premiers entre eux.

**7.** Soient $P$ et $Q$ les polynômes de $\mathbb{R}[X]$ définis par $P = 2X^4 - 2X^3 + 3X^2 - X + 1$ et $Q = X^4 - X^3 + 3X^2 - 2X + 2$.

**a)** Calculer le plus grand commun diviseur de $P$ et $Q$.

**b)** Factoriser $P$ et $Q$ en produit de polynômes irréductibles et unitaires de $\mathbb{R}[X]$.

**8.** Trouver les racines complexes du polynôme $X^2 - (3 + 4i)X - 1 + 7i$.

**9.** Soit $n$ un entier supérieur ou égal à 2. Posons $P = 1 + X + \frac{X^2}{2!} + \cdots + \frac{X^n}{n!}$.

**a)** Calculer $P - P'$.

**b)** Montrer que toutes les racines complexes de $P$ sont simples.

**10.** Soit $P$ le polynôme de $\mathbb{R}[X]$ défini par $P = 2X^5 + 5X^4 + 8X^3 + 7X^2 + 4X + 1$.

**a)** Combien le polynôme $P$ a-t-il de racines multiples dans $\mathbb{C}$ ?

**b)** Factoriser $P$ en produit de polynômes irréductibles et unitaires de $\mathbb{R}[X]$.

**11.** Soit $P$ un polynôme de $\mathbb{K}[X]$ de degré 3 et unitaire. Si $\alpha$, $\beta$ et $\gamma$ sont les racines complexes de $P$ et si $P = X^3 + aX^2 + bX + c$, montrer que l'on a $\alpha + \beta + \gamma = -a$, $\alpha\beta + \alpha\gamma + \beta\gamma = b$ et $\alpha\beta\gamma = -c$.

**12.** Soit $P$ le polynôme de $\mathbb{R}[X]$ défini par $P = X^4 + X^3 + X^2 + 3$.

**a)** Montrer que $P$ n'a pas de racine réelle.

**b)** Le polynôme $P$ est-il un polynôme irréductible de $\mathbb{R}[X]$ ?

**13. a)** Factoriser $X^4 + X^2 + 1$ et $X^4 - X^2 + 1$ en produit de polynômes irréductibles et unitaires de $\mathbb{R}[X]$.

**b)** Montrer que $X^4 - X^2 + 1$ est un polynôme irréductible de $\mathbb{Q}[X]$.

**14.** Soit $P$ le polynôme de $\mathbb{Q}[X]$ défini par $P = X^3 - X^2 - 2$.

**a)** Soient $p$ un entier relatif et $q$ un entier positif tels que $\text{pgcd}(p,q) = 1$. Montrer que si $p/q$ est racine de $P$, alors $q = 1$.

**b)** Montrer que $P$ n'a pas de racine rationnelle.

**c)** En déduire que $P$ est un polynôme irréductible de $\mathbb{Q}[X]$.

**15.** Soient $a, b \in \mathbf{K}$ et $P = X^4 + aX^3 + bX^2 + aX + 1$.

**a)** On suppose que 1 est racine de $P$. Montrer que $(X-1)^2$ divise $P$ et calculer le quotient de $P$ par $(X-1)^2$.

**b)** On suppose que $-1$ est racine de $P$. Montrer que $(X+1)^2$ divise $P$ et calculer le quotient de $P$ par $(X+1)^2$.

**16.** Soit $(P_n)$ la suite de polynômes de $\mathbb{Q}[X]$ définie par $P_0 = 2$, $P_1 = X$ et $P_{n+1} = XP_n - P_{n-1}$, pour tout entier positif $n$.

**a)** Calculer $P_2$ et $P_3$. Montrer que $P_n$ est un polynôme unitaire de degré $n$, si $n \geqslant 1$.

**b)** Montrer que pour tout $x \in \mathbb{C}$, $x \neq 0$, on a $x^n + \dfrac{1}{x^n} = P_n(y)$, où $y = x + \dfrac{1}{x}$.

**c)** Soient $a, b \in \mathbf{K}$ et $P = X^4 + aX^3 + bX^2 + aX + 1$. Montrer que pour tout $x \in \mathbb{C}$, $x \neq 0$, on a $P(x) = x^2(y^2 + ay + b - 2)$, où $y = x + \dfrac{1}{x}$.

**d)** Trouver les racines complexes du polynôme $X^4 - 2X^3 - X^2 - 2X + 1$.

**17.** Soient $a, b, c$ des nombres complexes, $P = X^3 + aX^2 + bX + c$ et $\alpha$, $\beta$, $\gamma$ les racines complexes de $P$. On considère le polynôme $Q = (X - \alpha^2)(X - \beta^2)(X - \gamma^2)$.

**a)** Montrer que $Q(X^2) = -P(X)P(-X)$. En déduire l'expression des coefficients de $Q$ en fonction de $a$, $b$ et $c$.

**b)** Calculer $Q$ lorsque $P = X^3 - X + 2$.

**18.** Soit $\alpha$ la racine cubique de l'unité de partie imaginaire strictement positive. Trouver un polynôme $P \in \mathbb{Q}[X]$ unitaire, de degré 4 et tel que $P(i + \alpha) = 0$. Quelles sont les racines complexes de $P$ ?

**19.** Notons $E$ l'espace vectoriel des polynômes à coefficients réels, nul ou de degré inférieur ou égal à 3. Soit $f : E \to E$ l'application qui à tout polynôme $P \in E$ associe le reste de la division euclidienne de $XP$ par $X^4 - X^2 - 1$.

**a)** Montrer que l'application $f$ est linéaire.

**b)** Écrire la matrice de $f$ dans la base $(1, X, X^2, X^3)$ de $E$.



**20.** Soit $f : \mathbb{R}[X] \to \mathbb{R}^4$ l'application définie par $f(P) = (P(1), P(2), P(3), P(4))$ pour tout $P \in \mathbb{R}[X]$.

**a)** Montrer que l'application $f$ est linéaire.

**b)** Soit $P \in \mathbb{R}[X]$. Montrer que $P$ appartient à $\operatorname{Ker} f$ si et seulement si le polynôme $P$ est multiple de $(X-1)(X-2)(X-3)(X-4)$.

**c)** Soit $E$ le sous-espace vectoriel de $\mathbb{R}[X]$ formé des polynômes nul ou de degré inférieur ou égal à 3 et soit $g : E \to \mathbb{R}^4$ l'application définie par $g(P) = f(P)$ pour tout $P \in E$. Montrer que l'application $g$ est linéaire et injective. En déduire que pour tous nombres réels $a, b, c, d$, il existe un unique polynôme $P \in E$ tel que $P(1) = a$, $P(2) = b$, $P(3) = c$ et $P(4) = d$.

**21.** Soient $a$ et $b$ des nombres réels. Pour tout entier positif $n$, on note $E_n$ le sous-espace vectoriel de $\mathbb{R}[X]$ formé des polynômes nul ou de degré strictement inférieur à $n$. On note $e_1, e_2, e_3, e_4, e_5$ les éléments suivants de $E_2 \times E_3$ :

$$e_1 = (1,0), \quad e_2 = (X,0), \quad e_3 = (0,1), \quad e_4 = (0,X), \quad e_5 = (0,X^2).$$

Soient $A$ un polynôme de degré 3 de $\mathbb{R}[X]$, $B$ un polynôme de degré 2 de $\mathbb{R}[X]$ et $f : E_2 \times E_3 \to E_5$ l'application définie par $f(P,Q) = AP + BQ$ pour tout $(P,Q) \in E_2 \times E_3$.

**a)** Calculer le déterminant de la matrice

$$\begin{bmatrix} b & 0 & a & 0 & 0 \\ a & b & 0 & a & 0 \\ 0 & a & 3 & 0 & a \\ 1 & 0 & 0 & 3 & 0 \\ 0 & 1 & 0 & 0 & 3 \end{bmatrix}.$$

**b)** Montrer que $(e_1, e_2, e_3, e_4, e_5)$ est une base de $E_2 \times E_3$.

**c)** Montrer que l'application $f$ est linéaire.

**d)** On suppose que les polynômes $A$ et $B$ ne sont pas premiers entre eux. Montrer que le polynôme constant 1 n'est pas dans l'image de $f$.

**e)** On suppose que les polynômes $A$ et $B$ sont premiers entre eux. Soit $(P,Q) \in \operatorname{Ker} f$. Montrer que $B$ divise $P$, puis que $P = Q = 0$.

**f)** Montrer que l'application $f$ est bijective si et seulement si les polynômes $A$ et $B$ sont premiers entre eux.

**g)** On suppose $A = X^3 + aX + b$ et $B = 3X^2 + a$. Calculer la matrice de $f$ dans les bases $(e_1, e_2, e_3, e_4, e_5)$ et $(1, X, X^2, X^3, X^4)$.

**h)** Montrer que le polynôme $X^3 + aX + b$ a des racines multiples dans $\mathbb{C}$ si et seulement si l'on a $4a^3 + 27b^2 = 0$.

**22. a)** Montrer que $X^3 - 2$ est un polynôme irréductible de $\mathbb{Q}[X]$. Quelles sont les racines complexes de $X^3 - 2$ ?

**b)** Soit $\alpha \in \mathbb{C}$ une racine de $X^3 - 2$.

(i) Soit $P \in \mathbb{Q}[X]$ un polynôme tel que $P(\alpha) = 0$. Montrer que $P$ est multiple de $X^3 - 2$.

(ii) Soient $p, q, r \in \mathbb{Q}$. Montrer que si $p + q\alpha + r\alpha^2 = 0$, alors $(p, q, r) = (0, 0, 0)$.

**23.** Cet exercice utilise le résultat de l'exercice 22.

Posons $\alpha = \sqrt[3]{2}$ et $j = -(1/2) + (\sqrt{3}/2)i$. Soient $p, q, r$ des entiers qui ne sont pas tous nuls et soit $P = p + qX + rX^2$. Posons $a = P(\alpha)$ et $b = P(j\alpha)P(j^2\alpha)$.

**a)** Calculer $j^3$ et $1 + j + j^2$.

**b)** Montrer que les nombres $a$ et $b$ sont différents de 0.

**c)** Montrer qu'il existe des entiers $u, v, w$ tels que $b = u + v\alpha + w\alpha^2$.

**d)** Calculer $ab$. En déduire que $ab$ est un entier.

**e)** Montrer que l'on a $\dfrac{1}{p + q\alpha + r\alpha^2} = \dfrac{p^2 - 2qr + (2r^2 - pq)\alpha + (q^2 - pr)\alpha^2}{p^3 + 2q^3 + 4r^3 - 6pqr}$.

## Quelques réponses ou indications

**4. a)** On a $X^n - a^n = (X^{kq} - a^{kq})X^r + a^{kq}X^r - a^{kq+r}$. D'autre part, $X - a^k$ divise $X^q - a^{kq}$, donc $X^k - a^k$ divise $X^{kq} - a^{kq}$.

**5. a)** Il existe $a, b \in \mathbb{R}$ tels que $R = aX + b$, donc $R = 0$ si et seulement si $R(i) = 0$.

**6. b)** Appliquer (a) pour montrer que le pgcd de ces polynômes est égal à 1.

**7. a)** $\mathrm{pgcd}(P, Q) = X^2 - X + 1$.

**b)** On a $P = (X^2 - X + 1)(2X^2 + 1)$ et $Q = (X^2 - X + 1)(X^2 + 2)$. Vérifier que ces facteurs de $P$ et $Q$ sont des polynômes irréductibles de $\mathbb{R}[X]$.

**8.** Se reporter au chapitre 3 pour trouver une racine carrée du discriminant.

**9. a)** On a $P - P' = \dfrac{X^n}{n!}$.

**b)** Si $P$ et $P'$ avaient une racine commune $a \in \mathbb{C}$, alors $a$ serait aussi racine de $P - P'$.

**12. a)** Étudier les variations de la fonction qui à tout $x \in \mathbb{R}$ associe $P(x)$.

**b)** Non car les polynômes irréductibles de $\mathbb{R}[X]$ sont ceux de degré 1 et ceux de degré 2 dont le discriminant est strictement négatif.

**13. b)** Procéder comme pour le polynôme $X^4 + 1$ qui a fait l'objet d'un exercice dans le cours.



**14. a)** Si $p/q$ est racine de $P$, on a $(p/q)^3 - (p/q)^2 - 2 = 0$. Multiplions cette égalité par $q^3$. Il vient $p^3 - pq - 2q^3 = 0$. On en déduit $q(p + 2q^2) = p^3$. Il s'ensuit que $q$ divise $p^3$ et donc $\mathrm{pgcd}(q, p^3) = q$. Puisque $q$ et $p$ sont premiers entre eux, $q$ et $p^3$ le sont également. Il s'ensuit $q = 1$.

**b)** Utiliser (a).

**15. a)** Le quotient est $X^2 + (a + 2)X + 1$.

**16. b)** Raisonner par récurrence.

**d)** Appliquer c).

**17. b)** La réponse est $Q = X^3 - 2X^2 + X - 4$.

**18.** On a $\alpha^3 = 1$ et $\alpha \neq 1$, donc $1 + \alpha + \alpha^2 = 0$. Poser $x = i + \alpha$ et montrer que l'on a $x^2 + x = i(1 + 2x)$. Le polynôme demandé est $P = (X^2 + X)^2 + (1 + 2X)^2$. Les racines de $P$ sont $i + \alpha$, $-i + \alpha$, $i + \bar{\alpha}$ et $-i + \bar{\alpha}$.

**19. b)** La matrice est $\begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$.

**20. c)** On a $\dim E = \dim \mathbb{R}^4$. L'application linéaire $g$ étant injective, elle est bijective.

**21. a)** Le déterminant est égal à $4a^3 + 27b^2$.

**e)** Utiliser le théorème de Gauss.

**f)** On a $\dim(E_2 \times E_3) = \dim E_5$, par suite l'application linéaire $f$ est bijective si et seulement si elle est injective, si et seulement si elle est surjective.

**g)** C'est la matrice de (a).

**h)** Les racines multiples de $X^3 + aX + b$ sont les racines complexes du plus grand commun diviseur de $X^3 + aX + b$ et de son polynôme dérivé, c'est-à-dire $3X^2 + a$. Utiliser alors (f), (g) et (a).

**22. a)** Voir un exercice traité dans le cours. Soit $j$ la racine cubique de l'unité de partie imaginaire strictement positive. Les racines complexes de $X^3 - 2$ sont $\sqrt[3]{2}$, $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$.

**b)** (i) Soit $D = \mathrm{pgcd}(P, X^3 - 2)$. Montrer que $\alpha$ est racine de $D$, donc $D$ n'est pas constant. Or $D$ divise le polynôme irréductible $X^3 - 2$. En déduire que $D = X^3 - 2$.

(ii) Appliquer (i) au polynôme $p + qX + rX^2$.

**23. a)** Le nombre complexe $j$ est une racine cubique de l'unité, donc $j^3 = 1$. Puisque $j \neq 1$, on en déduit l'égalité $1 + j + j^2 = 0$.

**b)** Utiliser le résultat de l'exercice précédent.

**d)** On a $ab = p^3 + 2q^3 + 4r^3 - 6pqr$.

# Chapitre 11

# Groupes

## 1. Définitions et règles de calcul

**Définition**

Soit $G$ un ensemble non vide. On dit que $G$ est un *groupe* s'il existe une opération dans $G$, notée $*$, ayant les propriétés suivantes :

- pour tous $x, y, z \in G$, on a $(x * y) * z = x * (y * z)$ et cet élément se note $x * y * z$
- il existe $e \in G$ tel que $e * x = x * e = x$ pour tout $x \in G$
- pour tout $x \in G$, il existe $x' \in G$ tel que $x * x' = x' * x = e$.

Soit $G$ un groupe. L'élément $e$ tel que $e * x = x * e = x$ pour tout $x \in G$ est unique et s'appelle l'*élément neutre* de $G$. En effet, si $e'$ est un élément de $G$ vérifiant la même propriété, il vient $e = e * e' = e'$.

Si $x$ est un élément de $G$, l'élément $x'$ tel que $x * x' = x' * x = e$ est unique et s'appelle le *symétrique* de $x$. En effet, si $x''$ est *a priori* un autre élément de $G$ tel que $x * x'' = x'' * x = e$, il vient $x' = x' * e = x' * (x * x'') = (x' * x) * x'' = e * x'' = x''$.

**Définition**

Soit $G$ un groupe. Si l'on a $x * y = y * x$ pour tous $x, y \in G$, on dit que le groupe $G$ est *commutatif*.

**Exemples**

1) Les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de l'addition sont des groupes commutatifs. L'élément neutre est 0 et le symétrique de $x$ est $-x$.

2) Les ensembles $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$ et $\mathbb{C} \setminus \{0\}$ munis du produit sont des groupes commutatifs. L'élément neutre est 1 et le symétrique de $x$ est $1/x$.

3) Si $\mathbf{K}$ est $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, un $\mathbf{K}$-espace vectoriel muni de l'addition est un groupe commutatif. L'élément neutre est le vecteur nul et le symétrique du vecteur $v$ est $-v$.

4) En particulier, si $\mathbb{K}$ est $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, l'ensemble des polynômes $\mathbb{K}[X]$ est un groupe commutatif, muni de l'addition. L'élément neutre est le polynôme nul et le symétrique du polynôme $P$ est $-P$.

5) Soit $n$ un entier supérieur ou égal à 2. Si $\mathbb{K}$ est $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, muni du produit, l'ensemble des matrices inversibles de $M_n(\mathbb{K})$ est un groupe non commutatif. Ce groupe s'appelle le *groupe linéaire* et se note $GL_n(\mathbb{K})$. L'élément neutre est la matrice $I_n$ et le symétrique de la matrice $A$ est $A^{-1}$. Au chapitre 5, nous avons vu qu'une matrice carrée est inversible si et seulement si son déterminant est non nul. Le groupe $GL_n(\mathbb{K})$ est donc l'ensemble des matrices de $M_n(\mathbb{K})$ de déterminant non nul.

6) Soit $E$ un ensemble non vide. Muni de la composition des applications, l'ensemble des bijections de $E$ sur $E$ est un groupe qui se note $\mathscr{S}(E)$. L'élément neutre est l'application identique $\mathrm{id}_E$ et le symétrique de l'application $f$ est la bijection réciproque $f^{-1}$. Nous verrons au paragraphe 4 que si l'ensemble $E$ a au moins trois éléments, le groupe $\mathscr{S}(E)$ n'est pas commutatif.

Dorénavant, lorsqu'on étudiera les propriétés d'un groupe $G$ général, l'élément $x * y$ sera noté plus simplement $xy$ et appelé le *produit* de $x$ par $y$. L'élément neutre sera noté 1 et le symétrique de $x$ sera noté $x^{-1}$.

Mais attention, cette notation multiplicative ne doit pas faire illusion. Comme nous l'avons vu dans les exemples (1), (3) et (4), l'opération dans un groupe peut être l'addition, notée alors $+$ et dans ce cas, l'élément neutre est noté 0 et le symétrique de $x$ est noté $-x$.

Remarquons que si $x, y$ sont des éléments de $G$ tels que $xy = 1$, alors on a $y = x^{-1}$, égalité qui s'obtient en multipliant à gauche par $x^{-1}$.

**Notation.** Soit $G$ un groupe. Pour tout $x \in G$, on pose $x^0 = 1$ et pour tout entier positif $n$, on note $x^n$ le produit de $x^{n-1}$ par $x$ ; de plus on pose $x^{-n} = (x^{-1})^n$.

Si $x$ est un élément d'un groupe $G$, on a pour tous entiers relatifs $n$ et $k$

$$x^n x^k = x^{n+k} \quad \text{et} \quad (x^n)^k = x^{nk}.$$

**Proposition.** *Soient $G$ un groupe et $x, y$ des éléments de $G$ tels que $xy = yx$. Alors on a $(xy)^n = x^n y^n$ pour tout entier positif $n$.*

**Démonstration.** Démontrons par récurrence que l'on a $xy^n = y^n x$ et $(xy)^n = x^n y^n$ pour tout entier positif $n$. Par hypothèse, la propriété est vraie lorsque $n = 1$. Soit $n$ un entier supérieur ou égal à 2. Supposons que la propriété est vraie pour l'entier $n-1$. Il vient $xy^n = (xy^{n-1})y = (y^{n-1}x)y = y^{n-1}(xy) = y^{n-1}(yx) = y^n x$ et $(xy)^n = (xy)^{n-1}xy = (x^{n-1}y^{n-1})xy = x^{n-1}(y^{n-1}x)y = x^{n-1}(xy^{n-1})y = x^n y^n$, ce qu'il fallait démontrer. ■



En plus des propriétés définissant un groupe $G$, voici deux règles utiles pour calculer dans $G$.

**Proposition.** *Soient $G$ un groupe et $x, y, z$ des éléments de $G$.*
- *On a les implications $(xy = xz) \Rightarrow y = z$ et $(yx = zx) \Rightarrow y = z$.*
- *On a $(xy)^{-1} = y^{-1}x^{-1}$.*

**Démonstration.** Si l'on a $xy = xz$, multiplions à gauche chaque membre de cette égalité par $x^{-1}$. Il vient $x^{-1}(xy) = x^{-1}(xz)$, ou encore $(x^{-1}x)y = (x^{-1}x)z$. Puisque $x^{-1}x = 1$, on en déduit $y = z$. Si $yx = zx$, alors en multipliant à droite chaque membre de cette égalité par $x^{-1}$, on obtient $y = z$, car $xx^{-1} = 1$.
On a $(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = x1x^{-1} = xx^{-1} = 1$. Il s'ensuit $(xy)^{-1} = y^{-1}x^{-1}$. ■

## 2. Sous-groupes

Soit $G$ un groupe.

**Définition**
Soit $H$ une partie de $G$. On dit que $H$ est un *sous-groupe* de $G$ si $1 \in H$ et si pour tous $x, y \in H$, on a $xy \in H$ et $x^{-1} \in H$.

Soit $H$ un sous-groupe de $G$ et soit $x \in H$. D'après la définition, le produit $xx = x^2$ appartient à $H$ et plus généralement, pour tout entier positif $k$, l'élément $x^k$ appartient à $H$. Puisque $1 \in H$ et $x^{-1} \in H$, on en déduit que pour tout entier $n \in \mathbb{Z}$, on a $x^n \in H$.

**Proposition.** *Soit $H$ un sous-groupe de $G$. Muni de la même opération que $G$, $H$ est un groupe.*

**Démonstration.** D'après les règles de calcul dans $G$, on a pour tous $x, y, z \in H$, $(xy)z = x(yz)$, $x1 = 1x = x$ et $x^{-1}x = xx^{-1} = 1$. Il s'ensuit que $H$ est un groupe. ■

Grâce à cette proposition, nous allons pouvoir obtenir de nombreux groupes.

**Exemple 1.** Le produit de deux nombres réels strictement positifs est strictement positif et l'inverse d'un nombre réel strictement positif est strictement positif. De plus 1 est un nombre réel strictement positif, donc $]0, +\infty[$ est un sous-groupe de $\mathbb{R} \setminus \{0\}$.

**Exemple 2.** Notons $\mathbb{U}$ l'ensemble des nombres complexes de module 1. Le nombre complexe 1 appartient à $\mathbb{U}$. Puisque $|zz'| = |z||z'|$ et $|1/z| = 1/|z|$, le produit de deux nombres complexes de module 1 est de module 1, ainsi que l'inverse d'un nombre complexe de module 1. Par suite $\mathbb{U}$ est un sous-groupe de $\mathbb{C} \setminus \{0\}$.

**Exemple 3.** Pour tout entier $n$ supérieur ou égal à 2, notons $\mathbf{U}_n$ l'ensemble des racines $n$-ièmes de l'unité, c'est-à-dire l'ensemble des nombres complexes $z$ tels que $z^n = 1$.
Si $z \in \mathbf{U}_n$, alors $|z|^n = 1$, donc $|z| = 1$. Il s'ensuit que $\mathbf{U}_n$ est une partie de $\mathbf{U}$. On a $1 \in \mathbf{U}_n$. De plus, si $a$ et $b$ sont des nombres complexes tels que $a^n = 1$ et $b^n = 1$, alors on a $(ab)^n = a^n b^n = 1$ et $\left(\frac{1}{a}\right)^n = \frac{1}{a^n} = 1$, donc $ab \in \mathbf{U}_n$ et $1/a \in \mathbf{U}_n$. Ainsi $\mathbf{U}_n$ est un sous-groupe de $\mathbf{U}$.
Au chapitre 3, nous avons vu que les éléments de $\mathbf{U}_n$ sont les nombres complexes de la forme $\cos(2k\pi/n) + i\sin(2k\pi/n)$, où $k$ est un entier compris entre 0 et $n-1$. Le groupe $\mathbf{U}_n$ a donc $n$ éléments.
Si l'on pose $\zeta = \cos(2\pi/n) + i\sin(2\pi/n)$, alors d'après la formule de Moivre, on a $\cos(2k\pi/n) + i\sin(2k\pi/n) = \zeta^k$. Les éléments du groupe $\mathbf{U}_n$ sont donc $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$.

**Exemple 4.** Soit $n$ un entier supérieur ou égal à 2. Si $\mathbf{K}$ est $\mathbf{Q}$, $\mathbf{R}$ ou $\mathbf{C}$, notons $\mathrm{SL}_n(\mathbf{K})$ l'ensemble des matrices de $M_n(\mathbf{K})$ de déterminant 1. Puisqu'une matrice de déterminant non nul est inversible, $\mathrm{SL}_n(\mathbf{K})$ est une partie de $\mathrm{GL}_n(\mathbf{K})$. On a $\det I_n = 1$, par suite $I_n$ appartient à $\mathrm{SL}_n(\mathbf{K})$. D'autre part, si $A, B$ sont des matrices de déterminant 1, il vient $\det(AB) = (\det A)(\det B) = 1$ et $\det(A^{-1}) = 1/\det A = 1$. On en déduit que $\mathrm{SL}_n(\mathbf{K})$ est un sous-groupe de $\mathrm{GL}_n(\mathbf{K})$.

**Exemple 5.** Soit $n$ un entier supérieur ou égal à 2. Au chapitre 8, nous avons défini les homothéties et les translations : ce sont des bijections de $\mathbf{R}^n$ dans $\mathbf{R}^n$. La bijection réciproque de la translation de vecteur $v$ est la translation de vecteur $-v$. La bijection réciproque de l'homothétie de centre $O$ et de rapport $k \neq 0, 1$ est l'homothétie de centre $O$ et de rapport $1/k$. De plus, nous avons montré que la composée de deux translations est une translation, que la composée de deux homothéties est ou bien une homothétie, ou bien une translation et enfin que la composée d'une translation et d'une homothétie est une homothétie. Puisque l'application identique de $\mathbf{R}^n$ est la translation de vecteur nul, il s'ensuit que l'ensemble des homothéties et translations est un sous-groupe du groupe $\mathscr{S}(\mathbf{R}^n)$.

**Exemple 6.** Si $a \in \mathbf{N}$, notons $a\mathbf{Z}$ l'ensemble des entiers relatifs multiples de $a$. L'ensemble $a\mathbf{Z}$ est un sous-groupe de $\mathbf{Z}$. En effet, 0 est multiple de $a$ et si $x$ et $y$ des entiers relatifs multiples de $a$, alors $x + y$ et $-x$ sont multiples de $a$.

Dans l'exemple 6, nous venons en fait de trouver tous les sous-groupes de $\mathbf{Z}$ : c'est ce qu'affirme la proposition suivante.

**Proposition.** *Une partie $H$ de $\mathbf{Z}$ est un sous-groupe de $\mathbf{Z}$ si et seulement s'il existe $a \in \mathbf{N}$ tel que $H = a\mathbf{Z}$.*



**Démonstration.** Il suffit de démontrer que tout sous-groupe de $\mathbf{Z}$ est de la forme $a\mathbf{Z}$. Supposons que $H$ est un sous-groupe de $\mathbf{Z}$. Si $H = \{0\}$, alors $H = 0\mathbf{Z}$.
Supposons $H \neq \{0\}$. Il existe donc un élément $h \in H$ tel que $h \neq 0$. Puisque $H$ est un sous-groupe de $\mathbf{Z}$, on a aussi $-h \in H$, donc le plus grand des deux entiers $h$ et $-h$ appartient à $H$. Cet entier $|h| = \max(h, -h)$ est positif. Puisqu'il n'y a qu'un nombre fini d'entiers positifs inférieurs ou égaux à $|h|$, il existe dans $H$ un plus petit entier positif. Notons-le $a$. Puisque $H$ est un sous-groupe de $\mathbf{Z}$ contenant l'entier $a$, $H$ contient tous les multiples de $a$. On a donc l'inclusion $a\mathbf{Z} \subset H$.
Soit $x \in H$. Notons $q$ le quotient et $r$ le reste de la division euclidienne de $x$ par $a$, de sorte que l'on a $x = aq + r$ et $0 \leqslant r < a$. Puisque $x$ et $aq$ appartiennent à $H$, $x - aq \in H$. On a donc $r \in H$ et $0 \leqslant r < a$. Par définition de $a$, il s'ensuit $r = 0$. L'entier $x$ est donc multiple de $a$, autrement dit $x \in a\mathbf{Z}$. Nous avons ainsi montré que tout élément de $H$ appartient à $a\mathbf{Z}$, c'est-à-dire que l'on a $H \subset a\mathbf{Z}$. Cela prouve l'égalité $H = a\mathbf{Z}$. ∎

## 3. Homomorphismes

**Définition**

Soient $G$ et $G'$ des groupes. Notons $*$ l'opération dans $G$ et $*'$ l'opération dans $G'$. Un *homomorphisme de $G$ dans $G'$* est une application $f : G \to G'$ telle que $f(x * y) = f(x) *' f(y)$ pour tous $x, y \in G$.

**Exemple 1.** La fonction exponentielle est un homomorphisme du groupe $\mathbf{R}$ muni de l'addition dans le groupe $\mathbf{R} \setminus \{0\}$ muni du produit. En effet, puisque $\exp x$ n'est jamais nul, cette fonction prend bien ses valeurs dans l'ensemble $\mathbf{R} \setminus \{0\}$, et l'on a $\exp(x + y) = (\exp x)(\exp y)$ pour tous nombres réels $x$ et $y$.

**Exemple 2.** Soit $n$ un entier supérieur ou égal à 2. Dans l'exemple 3, nous avons montré que l'ensemble $\mathbf{U}_n$ des racines $n$-ièmes de l'unité forme un groupe pour la multiplication. Posons $\zeta = \cos(2\pi/n) + i\sin(2\pi/n)$, de sorte que l'on a $\zeta \in \mathbf{U}_n$.
Soit $f : \mathbf{Z} \to \mathbf{U}_n$ l'application définie par $f(k) = \zeta^k$ pour tout $k \in \mathbf{Z}$. Alors $f$ est un homomorphisme. En effet, pour tous entiers $k, k' \in \mathbf{Z}$, on a $f(k+k') = \zeta^{k+k'} = \zeta^k \zeta^{k'} = f(k)f(k')$.
Dans l'exemple déjà cité, nous avons aussi montré que l'on a $\mathbf{U}_n = \{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}$. Le groupe $\mathbf{U}_n$ est donc constitué seulement des puissances de $\zeta$ d'exposant inférieur à $n$.
En fait, pour tout entier $k \in \mathbf{Z}$, on a $\zeta^k = \zeta^r$, où $r$ est le reste de la division euclidienne de $k$ par $n$ : en effet, on a $k = nq + r$, donc $\zeta^k = \zeta^{nq+r} = (\zeta^n)^q \zeta^r = \zeta^r$ car $\zeta^n = 1$.

**Proposition.** *Soient $G, G'$ des groupes et $f$ un homomorphisme de $G$ dans $G'$. Alors on a $f(1) = 1$ et $f(x^{-1}) = \big(f(x)\big)^{-1}$ pour tout $x \in G$.*

**Démonstration.** Dans $G$, on a $1^2 = 1$. Il s'ensuit $f(1^2) = f(1)$. Puisque $f$ est un homomorphisme de $G$ dans $G'$, on a $f(1^2) = \big(f(1)\big)^2$. Il vient donc $1\,f(1) = f(1)f(1)$. En simplifiant cette égalité par $f(1)$, ce qui est permis d'après la dernière proposition du paragraphe 1, nous obtenons $f(1) = 1$.
Soit $x \in G$. On a $xx^{-1} = 1$, donc $f(xx^{-1}) = f(1) = 1$. Puisque $f$ est un homomorphisme de $G$ dans $G'$, on en déduit $f(x)f(x^{-1}) = 1$. L'élément $f(x^{-1})$ est donc le symétrique de $f(x)$ dans $G'$. ■

**Proposition.** *Soient $G, G', G''$ des groupes, $f$ un homomorphisme de $G$ dans $G'$ et $f'$ un homomorphisme de $G'$ dans $G''$. Alors le composé $f' \circ f$ est un homomorphisme de $G$ dans $G''$.*

**Démonstration.** Soient $x$ et $y$ des éléments de $G$. On a $f(xy) = f(x)f(y)$, par suite $f' \circ f(xy) = f'\big(f(xy)\big) = f'\big(f(x)f(y)\big) = f'\big(f(x)\big)f'\big(f(y)\big)$. ■

**Définition**
Soient $G$ et $G'$ des groupes. Un *isomorphisme de $G$ sur $G'$* est un homomorphisme de $G$ dans $G'$ qui est de plus une application bijective.

**Exemple.** La fonction logarithme est un isomorphisme du groupe $]0, +\infty[$ muni du produit sur le groupe $\mathbb{R}$ muni de l'addition. En effet, la fonction Log est une bijection de $]0, +\infty[$ dans $\mathbb{R}$ et l'on a $\mathrm{Log}(xy) = \mathrm{Log}\,x + \mathrm{Log}\,y$ pour tous nombres réels $x, y$ strictement positifs.

Puisqu'une composée de bijections est une bijection, on en déduit qu'un composé d'isomorphismes est un isomorphisme.

**Proposition.** *Soient $G, G'$ des groupes et $f : G \to G'$ un isomorphisme. La bijection réciproque $f^{-1}$ est un isomorphisme de $G'$ sur $G$.*

**Démonstration.** Au chapitre 2, nous avons montré que $f^{-1}$ est une application bijective. Il suffit donc de démontrer que $f^{-1}$ est un homomorphisme de $G'$ dans $G$. Soient $x', y' \in G'$. Puisque $f$ est un homomorphisme de $G$ dans $G'$, on a $f\big(f^{-1}(x')f^{-1}(y')\big) = f\big(f^{-1}(x')\big)f\big(f^{-1}(y')\big)$. D'autre part, par définition de la bijection réciproque, on a $f\big(f^{-1}(x')\big) = x'$, $f\big(f^{-1}(y')\big) = y'$ et $x'y' = f\big(f^{-1}(x'y')\big)$. On en déduit $f\big(f^{-1}(x')f^{-1}(y')\big) = x'y' = f\big(f^{-1}(x'y')\big)$. L'application $f$ étant injective, il s'ensuit $f^{-1}(x')f^{-1}(y') = f^{-1}(x'y')$. L'application $f^{-1}$ est donc un homomorphisme de $G'$ dans $G$. ■

**Définition**
On dit que les groupes $G$ et $G'$ sont *isomorphes* s'il existe un isomorphisme de $G$ sur $G'$.



**Exercice.** Soient $X$ et $Y$ des ensembles tels qu'il existe une bijection $u : X \to Y$.
a) Soit $s \in \mathscr{S}(X)$. Démontrer que $u \circ s \circ u^{-1} \in \mathscr{S}(Y)$.
b) Soit $f : \mathscr{S}(X) \to \mathscr{S}(Y)$ l'application définie par $f(s) = u \circ s \circ u^{-1}$ pour tout $s \in \mathscr{S}(X)$. Montrer que $f$ est un homomorphisme.
c) Montrer que les groupes $\mathscr{S}(X)$ et $\mathscr{S}(Y)$ sont isomorphes.

**Réponse**
a) L'application $u \circ s \circ u^{-1}$ a $Y$ comme ensemble de départ et d'arrivée. D'autre part, $u \circ s \circ u^{-1}$ est la composée de trois bijections, donc est une bijection. Ainsi $u \circ s \circ u^{-1}$ est une bijection de $Y$ sur $Y$, c'est-à-dire un élément de $\mathscr{S}(Y)$.
b) Soient $s$ et $s'$ des éléments de $\mathscr{S}(X)$. Il vient

$$\begin{aligned} f(s) \circ f(s') &= (u \circ s \circ u^{-1}) \circ (u \circ s' \circ u^{-1}) = u \circ s \circ (u^{-1} \circ u) \circ s' \circ u^{-1} \\ &= u \circ s \circ \mathrm{id}_X \circ s' \circ u^{-1} = u \circ s \circ s' \circ u^{-1} = f(s \circ s'). \end{aligned}$$

L'application $f$ est donc un homomorphisme.
c) Comme en (a), si $t \in \mathscr{S}(Y)$, alors $u^{-1} \circ t \circ u \in \mathscr{S}(X)$. Notons $g$ l'application de $\mathscr{S}(Y)$ dans $\mathscr{S}(X)$ qui à tout élément $t \in \mathscr{S}(Y)$ associe $u^{-1} \circ t \circ u$. Si $s \in \mathscr{S}(X)$, nous avons

$$\begin{aligned} g \circ f(s) &= g(u \circ s \circ u^{-1}) = u^{-1} \circ (u \circ s \circ u^{-1}) \circ u \\ &= (u^{-1} \circ u) \circ s \circ (u^{-1} \circ u) = \mathrm{id}_X \circ s \circ \mathrm{id}_X = s. \end{aligned}$$

Il vient donc $g \circ f = \mathrm{id}_{\mathscr{S}(X)}$. De même, on démontre que $f \circ g = \mathrm{id}_{\mathscr{S}(Y)}$. Il s'ensuit que $f$ est une application bijective. L'application $f$ est donc un isomorphisme de $\mathscr{S}(X)$ sur $\mathscr{S}(Y)$, par suite les groupes $\mathscr{S}(X)$ et $\mathscr{S}(Y)$ sont isomorphes.

## 4. Le groupe symétrique

Soit $n$ un entier supérieur ou égal à 2. Notons $\{1, 2, \ldots, n\}$ l'ensemble des $n$ premiers entiers positifs.

**Définitions**
Le groupe des bijections de l'ensemble $\{1, 2, \ldots, n\}$ dans lui-même s'appelle le *groupe symétrique* et se note $\mathscr{S}_n$. Un élément de $\mathscr{S}_n$ s'appelle une *permutation*.

Puisqu'un ensemble $X$ à $n$ éléments est en bijection avec $\{1, 2, \ldots, n\}$, le groupe $\mathscr{S}(X)$ est, d'après l'exercice précédent, isomorphe à $\mathscr{S}_n$. Cela justifie l'étude du groupe symétrique.
Au paragraphe 4 du chapitre 2, nous avons montré que $\mathscr{S}_n$ possède $n!$ éléments. Par exemple, le groupe $\mathscr{S}_3$ a six éléments.
L'opération du groupe $\mathscr{S}_n$ est la composition des applications. L'usage est de noter $ss'$ l'élément $s \circ s'$ et de l'appeler le produit de $s$ par $s'$. De plus, nous noterons id l'élément neutre de $\mathscr{S}_n$ et nous l'appellerons *l'identité de $\mathscr{S}_n$*. Autrement dit, id est l'application identique de l'ensemble $\{1, 2, \ldots, n\}$.

### Définition

Soit $s$ une permutation. On dit que $s$ est une *transposition* s'il existe deux entiers $i$ et $j$, différents et appartenant à $\{1, 2, \ldots, n\}$, tels que

$$\begin{cases} s(i) = j \\ s(j) = i \\ s(k) = k \quad \text{pour tout } k \neq i, j. \end{cases}$$

Une transposition est donc une bijection qui échange deux entiers et qui laisse fixes tous les autres. On note $(i\ j)$ la transposition qui échange $i$ et $j$. Ainsi l'on a $(i\ j)=(j\ i)$.

### Le groupe $\mathscr{S}_3$

Les transpositions appartenant à $\mathscr{S}_3$ sont $(1\ 2)$, $(1\ 3)$ et $(2\ 3)$. Soit $s$ la permutation de $\mathscr{S}_3$ définie par $s(1)=2$, $s(2)=3$, $s(3)=1$. L'image de 1 par $s$ est 2, l'image de 2 est 3 et celle de 3 est 1. Il y a une notation commode pour écrire cela : $s=(1\ 2\ 3)$. Puisque le produit de $s$ par lui-même est la composée de $s$ par $s$, il vient

$$\begin{cases} s^2(1) = s\big(s(1)\big) = s(2) = 3 \\ s^2(2) = s\big(s(2)\big) = s(3) = 1 \\ s^2(3) = s\big(s(3)\big) = s(1) = 2 \end{cases}$$

donc l'image de 1 par $s^2$ est 3, l'image de 3 est 2 et celle de 2 est 1. De même on écrit $s^2 = (1\ 3\ 2)$. Posons $t = (1\ 2)$. Nous avons

$$(st)(1) = s\big(t(1)\big) = s(2) = 3 \quad \text{et} \quad st(2) = s\big(t(2)\big) = s(1) = 2.$$

Puisque $st$ est une bijection de $\{1, 2, 3\}$ dans lui-même, on en déduit $(st)(3) = 1$. Il s'ensuit $st = (1\ 3)$. Un calcul analogue montre que l'on a $ts = (2\ 3)$. Les six éléments du groupe $\mathscr{S}_3$ sont donc id, $s$, $s^2$, $t$, $st$ et $ts$.

Nous allons généraliser la notation que nous avons employée pour une transposition et pour les éléments de $\mathscr{S}_3$.

### Définition

Soit $p$ un entier tel que $2 \leqslant p \leqslant n$ et soit $s \in \mathscr{S}_n$. On dit que $s$ est un *$p$-cycle* s'il existe $p$ éléments $a_1, a_2, \ldots, a_p$ de $\{1, 2, \ldots, n\}$, deux à deux différents, tels que

$$\begin{cases} s(a_i) = a_{i+1} & \text{pour tout entier } i < p \\ s(a_p) = a_1 \\ s(j) = j & \text{pour tout } j \notin \{a_1, a_2, \ldots, a_p\}. \end{cases}$$

Cette permutation $s$ se note $(a_1\ a_2\ \cdots\ a_p)$.



**Exemple.** Soit $s$ la permutation de $\mathscr{S}_4$ définie par

$$s(1) = 3, \quad s(2) = 1, \quad s(3) = 4 \quad \text{et } s(4) = 2.$$

On a alors $s = (1\ 3\ 4\ 2)$, mais on a aussi $s = (4\ 2\ 1\ 3)$. La permutation $s$ est un 4-cycle. L'inverse de $s$ est le 4-cycle $s^{-1} = (2\ 4\ 3\ 1)$.

On a $s^2(1) = s(3) = 4$ et $s^2(4) = s(2) = 1$, donc $s^2$ n'est pas un 4-cycle. Mais on a $s^3(1) = 2$, $s^3(2) = 4$, $s^3(4) = 3$ et $s^3(3) = 1$, donc $s^3$ est le 4-cycle $(1\ 2\ 4\ 3)$. En fait, nous avons $s^3 = s^{-1}$, d'où en multipliant par $s$, l'égalité $s^4 = \text{id}$.

**Proposition.** *Si $s$ est un $p$-cycle, alors on a $s^p = \text{id}$.*

**Démonstration.** Écrivons $s = (a_1\ a_2\ \cdots\ a_p)$ et démontrons par récurrence que pour tout entier $k$ tel que $0 \leqslant k \leqslant p-1$, on a $s^k(a_1) = a_{k+1}$. Puisque $s^0 = \text{id}$, la propriété est vraie pour $k = 0$. Soit $k$ un entier tel que $1 \leqslant k \leqslant p-1$. Supposons que l'on a $s^{k-1}(a_1) = a_k$. Il vient $s^k(a_1) = s\big(s^{k-1}(a_1)\big) = s(a_k) = a_{k+1}$, ce qui achève la démonstration. En particulier, on a $s^{p-1}(a_1) = a_p$, par suite $s^p(a_1) = s\big(s^{p-1}(a_1)\big) = s(a_p) = a_1$. Si $k$ est un entier tel que $1 \leqslant k \leqslant p$, il vient

$$s^p(a_k) = s^p\big(s^{k-1}(a_1)\big) = s^{p+k-1}(a_1) = s^{k-1}\big(s^p(a_1)\big) = s^{k-1}(a_1) = a_k.$$

On a donc démontré que pour tout entier $k$ tel que $1 \leqslant k \leqslant p$, on a $s^p(a_k) = a_k$. Enfin, si $j$ est un entier de $\{1, 2, \ldots, n\}$ différent de tous les $a_i$, alors $s(j) = j$ et donc $s^p(j) = j$. Il s'ensuit $s^p = \text{id}$. ∎

### Définition

Soit $s$ une permutation. On dit que $s$ est un *cycle* s'il existe un entier $p$ compris entre 2 et $n$ tel que $s$ est un $p$-cycle.

### Remarques

- L'inverse d'un $p$-cycle est un $p$-cycle : par exemple pour un 3-cycle $(a\ b\ c)$, on a $(a\ b\ c)^{-1} = (c\ b\ a)$.
- Un produit de cycles n'est pas forcément un cycle. Par exemple, le produit $t = (1\ 2)(3\ 4)$ n'est pas un cycle, car pour tout $j \in \{1, 2, 3, 4\}$, on a $t^2(j) = j$. Mais si l'on pose $s = (1\ 2)(2\ 3)(3\ 4)$, alors il vient $s(1) = 2$, $s(2) = 3$, $s(3) = 4$ et $s(4) = 1$, donc $s = (1\ 2\ 3\ 4)$.

### Définition

Soient $p$ et $q$ des entiers compris entre 2 et $n$. On dit que les cycles $(a_1\ a_2\ \cdots\ a_p)$ et $(b_1\ b_2\ \cdots\ b_q)$ sont *à supports disjoints* si les ensembles $\{a_1, a_2, \ldots, a_p\}$ et $\{b_1, b_2, \ldots, b_q\}$ ont une intersection vide.

**Exemple.** Dans $\mathscr{S}_5$, les cycles $(1\ 4\ 5)$ et $(2\ 3)$ sont à supports disjoints, alors que les cycles $(1\ 2\ 5)$ et $(2\ 3\ 4)$ ne le sont pas.

**Proposition.** *Si $s$ et $t$ sont des cycles à supports disjoints du groupe $\mathscr{S}_n$, alors on a $st=ts$.*

**Démonstration.** Écrivons $s=(a_1\ a_2\ \cdots\ a_p)$ et $t=(b_1\ b_2\ \cdots\ b_q)$. Puisque $\{a_1,a_2,\ldots,a_p\}\cap\{b_1,b_2,\ldots,b_q\}=\varnothing$, on a $t(a_i)=a_i$ pour tout $i\in\{1,2,\ldots,p\}$ et $s(b_j)=b_j$ pour tout $j\in\{1,2,\ldots,q\}$. Si $i\in\{1,\ldots,p-1\}$, on a donc $ts(a_i)=t(s(a_i))=t(a_{i+1})=a_{i+1}$ et $(st)(a_i)=s(t(a_i))=s(a_i)=a_{i+1}$. D'autre part, on a $(ts)(a_p)=t(s(a_p))=t(a_1)=a_1$ et $(st)(a_p)=s(t(a_p))=s(a_p)=a_1$. Il s'ensuit $(ts)(a_i)=(st)(a_i)$ pour tout $i\in\{1,2,\ldots,p\}$. De même, on démontre que l'on a $(ts)(b_j)=(st)(b_j)$ pour tout $j\in\{1,2,\ldots,q\}$. Enfin, si $k\in\{1,2,\ldots,n\}$ est différent de tous les $a_i$ et de tous les $b_j$, alors on a $s(k)=k$, $t(k)=k$ et par conséquent $(st)(k)=(ts)(k)=k$. Les applications $st$ et $ts$ sont donc égales. ∎

**Théorème.** *Tout élément du groupe $\mathscr{S}_n$, différent de l'identité, est produit de cycles à supports disjoints.*

Admettons ce théorème et voyons sur un exemple comment on obtient pratiquement une telle décomposition.

**Exemple.** Soit $s$ la permutation de $\mathscr{S}_8$ définie par

$$s(1)=8 \quad s(3)=5 \quad s(5)=1 \quad s(7)=4$$
$$s(2)=2 \quad s(4)=6 \quad s(6)=7 \quad s(8)=3.$$

Calculons les images successives de 1 : on a $s(1)=8$, $s(8)=3$, $s(3)=5$ et $s(5)=1$. Dans la décomposition de $s$ en cycles à supports disjoints, il apparaît le 4-cycle $(1\ 8\ 3\ 5)$. Calculons maintenant les images successives de 2 : on a $s(2)=2$, donc 2 ne figure pas dans les cycles cherchés. Le premier entier qui n'est pas encore apparu est 4 : on a $s(4)=6$, $s(6)=7$ et $s(7)=4$. Puisqu'on a épuisé tous les entiers entre 1 et 8, on en déduit la décomposition $s=(1\ 8\ 3\ 5)(4\ 6\ 7)$. D'après la proposition précédente, nous avons aussi $s=(4\ 6\ 7)(1\ 8\ 3\ 5)$. Mais nous pouvons également écrire $s=(6\ 7\ 4)(3\ 5\ 1\ 8)$.

Puisque des cycles à supports disjoints commutent deux à deux, la décomposition d'une permutation $s$ en produit de cycles à supports disjoints permet de calculer toutes les puissances de $s$, en utilisant la proposition page 248.

**Exercice.** Soit $s$ la permutation de $\mathscr{S}_9$ définie par $s=(1\ 9)(3\ 4\ 8)(2\ 9\ 5\ 7)(2\ 6\ 7)$.

a) Décomposer $s$ en produit de cycles à supports disjoints.

b) Calculer $s^{1000}$.



**Réponse**

a) On obtient $s=(1\ 9\ 5\ 7)(2\ 6)(3\ 4\ 8)$.

b) Puisque les cycles $(1\ 9\ 5\ 7)$, $(2\ 6)$ et $(3\ 4\ 8)$ commutent deux à deux, on a $s^{1000}=(1\ 9\ 5\ 7)^{1000}(2\ 6)^{1000}(3\ 4\ 8)^{1000}$. Puisque $(1\ 9\ 5\ 7)$ est un 4-cycle, on a $(1\ 9\ 5\ 7)^4=\mathrm{id}$. De même on a $(2\ 6)^2=\mathrm{id}$ et $(3\ 4\ 8)^3=\mathrm{id}$. On en déduit les égalités

$$(1\ 9\ 5\ 7)^{1000}=\left((1\ 9\ 5\ 7)^4\right)^{250}=\mathrm{id}$$
$$(2\ 6)^{1000}=\left((2\ 6)^2\right)^{500}=\mathrm{id}$$
$$(3\ 4\ 8)^{1000}=\left((3\ 4\ 8)^3\right)^{333}(3\ 4\ 8)=\mathrm{id}\,(3\ 4\ 8)=(3\ 4\ 8).$$

Ainsi on a $s^{1000}=(3\ 4\ 8)$.

**Théorème.** *Tout élément du groupe $\mathscr{S}_n$ est produit de transpositions.*

**Démonstration.** On a $(1\ 2)^2=\mathrm{id}$ donc l'identité est bien un produit de transpositions. Démontrons par récurrence sur $p$ qu'un $p$-cycle est produit de transpositions. Puisqu'un 2-cycle est une transposition, la propriété est vraie lorsque $p=2$. Supposons l'entier $p$ supérieur ou égal à 3 et la propriété vraie pour l'entier $p-1$. Soit $s=(a_1\ a_2\ \cdots\ a_p)$ un $p$-cycle. Nous avons $s=(a_1\ a_2)(a_2\ a_3\ \cdots\ a_p)$. Par hypothèse de récurrence, le $(p-1)$-cycle $(a_2\ a_3\ \cdots\ a_p)$ est produit de transpositions, par suite $s$ l'est aussi. On a donc démontré que tout cycle de $\mathscr{S}_n$ est produit de transpositions. Puisque tout élément de $\mathscr{S}_n$ différent de id est produit de cycles, on en déduit que tout élément de $\mathscr{S}_n$ différent de id est produit de transpositions. ∎

## Exercices

1. Soit $G$ un groupe et soient $a$ et $b$ des éléments de $G$ tels que $a^5=1$ et $a^3b=ba^3$.
   a) Montrer que l'on a $a^6b=ba^6$.
   b) En déduire que l'on a $ab=ba$.
2. Soit $G$ un groupe. On suppose que pour tout $x\in G$, on a $x^2=1$.
   a) Montrer que l'on a $x=x^{-1}$ pour tout $x\in G$.
   b) Montrer que le groupe $G$ est commutatif.
3. Soit $G$ un groupe. Posons $H=\{x\in G \mid xy=yx, \forall y\in G\}$.
   a) Montrer que $H$ est un sous-groupe de $G$.
   b) Montrer que $H$ est un groupe commutatif.
4. Posons $\omega=\cos\frac{\pi}{3}+i\sin\frac{\pi}{3}$.
   a) Calculer $\omega^3$ et $\omega^6$.

**b)** Montrer que les nombres complexes $1, \omega, \omega^2, \omega^3, \omega^4$ et $\omega^5$ sont deux à deux différents. Dorénavant, posons $G = \{1, \omega, \omega^2, \omega^3, \omega^4, \omega^5\}$, $K = \{1, \omega^2, \omega^4\}$ et $L = \{1, \omega^3\}$.

**c)** Montrer que $G$ est un sous-groupe de $\mathbb{C} \setminus \{0\}$. Quel est le symétrique de $\omega$ ?

**d)** Montrer que $K$ et $L$ sont des sous-groupes de $G$.

**e)** Soit $H$ un sous-groupe de $G$ différent de $\{1\}$ et ne contenant ni $\omega$, ni $\omega^5$. Montrer que l'on a $H = K$ ou bien $H = L$.

**f)** Déterminer tous les sous-groupes de $G$.

**5.** Déterminer tous les sous-groupes du groupe $\mathscr{S}_3$.

**6.** Pour tous nombres $a, b \in \mathbb{C}$, $a \neq 0$, on définit l'application $f_{a,b} : \mathbb{C} \to \mathbb{C}$ en posant $f_{a,b}(z) = az + b$.

**a)** Soient $a, b \in \mathbb{C}$ tels que $a \neq 0$. Montrer que l'application $f_{a,b}$ est bijective.

**b)** Soit $G$ l'ensemble des $f_{a,b}$ où $a, b \in \mathbb{C}$ et $a \neq 0$. Montrer que $G$ est un sous-groupe de $\mathscr{S}(\mathbb{C})$. Montrer que le groupe $G$ n'est pas commutatif.

**7.** Soit $f : \mathbb{C} \setminus \{0\} \to \mathbb{U}$ l'application définie par $f(z) = z/|z|$. Montrer que $f$ est un homomorphisme surjectif.

**8.** Soit $f : \mathbb{U} \to \mathbb{U}$ l'application définie par $f(z) = z^2$. Montrer que $f$ est un homomorphisme surjectif.

**9. a)** Soit $a \in \mathbb{Q}$. Montrer que pour tout entier positif $n$, il existe un élément $b \in \mathbb{Q}$ tel que $nb = a$.

**b)** En déduire que les groupes $\mathbb{Z}$ et $\mathbb{Q}$ munis de l'addition ne sont pas isomorphes.

**10.** Rappelons que pour tout entier $n \geqslant 2$, on note $\mathbb{U}_n$ le groupe des racines $n$-ièmes de l'unité. Soit $n$ un entier supérieur ou égal à 2 et soit $d$ un diviseur de $n$ tel que $d \geqslant 2$.

**a)** Montrer que $\mathbb{U}_d$ est un sous-groupe de $\mathbb{U}_n$.

**b)** Posons $\zeta = \cos(2\pi/15) + i\sin(2\pi/15)$. Quelles sont les puissances de $\zeta$ qui appartiennent à $\mathbb{U}_3$ ?

**c)** Soit $k$ le quotient de $n$ par $d$. Supposons que l'on a $k \geqslant 2$. Montrer que l'application $f : \mathbb{U}_n \to \mathbb{C}$ définie par $f(z) = z^k$ prend ses valeurs dans $\mathbb{U}_d$ et définit un homomorphisme surjectif du groupe $\mathbb{U}_n$ dans le groupe $\mathbb{U}_d$.

**11. a)** Soient $x$ et $y$ des nombres réels différents de 1. Montrer que $x + y - xy$ est différent de 1.

**b)** Pour tous nombres $x, y \in \mathbb{R} \setminus \{1\}$, posons $x * y = x + y - xy$. Montrer que l'ensemble $\mathbb{R} \setminus \{1\}$, muni de l'opération $*$, est un groupe commutatif.

**c)** Soit $f : \mathbb{R} \setminus \{0\} \to \mathbb{R} \setminus \{1\}$ l'application définie par $f(x) = 1 - (1/x)$. On munit l'ensemble $\mathbb{R} \setminus \{0\}$ de la multiplication et l'ensemble $\mathbb{R} \setminus \{1\}$ de l'opération $*$. Montrer que $f$ est un isomorphisme.



**12.** Soit $G$ un groupe. Pour tout élément $g \in G$, notons $m_g$ l'application de $G$ dans $G$ définie par $m_g(x) = gx$ pour tout $x \in G$.

**a)** Soit $g \in G$. Montrer que l'application $m_g$ est bijective.

**b)** Soit $\varphi : G \to \mathscr{S}(G)$ l'application définie par $\varphi(g) = m_g$ pour tout $g \in G$. Montrer que $\varphi$ est un homomorphisme injectif.

**13.** Soit $n$ un entier au moins égal à 2 et soit $f : \mathrm{GL}_n(\mathbb{R}) \to \mathrm{GL}_n(\mathbb{R})$ l'application définie par $f(M) = {}^t(M^{-1})$. Montrer que $f$ est un isomorphisme de groupes.

**14.** Soit $n$ un entier supérieur ou égal à 2. Soient $t = (i\ j)$ une transposition de $\mathscr{S}_n$ et $s$ un élément de $\mathscr{S}_n$.

**a)** Montrer que $s(i) \neq s(j)$.

**b)** Montrer que $st(s^{-1})$ est la transposition de $\mathscr{S}_n$ qui échange $s(i)$ et $s(j)$.

**15.** Soit $H$ la partie de $\mathscr{S}_4$ définie par $H = \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.

**a)** Soit $s \in H$. Montrer que l'on a $s^2 = \mathrm{id}$.

**b)** Montrer que $H$ est un sous-groupe de $\mathscr{S}_4$.

**c)** Soit $s \in \mathscr{S}_4$ et soit $t \in H$. Montrer que $st(s^{-1})$ appartient à $H$.

**16.** Notons $s$ l'élément $(1\ 2\ 3\ 4)$ de $\mathscr{S}_4$.

**a)** Décomposer $s^2$ et $s^3$ en produit de cycles à supports disjoints.

**b)** Montrer que les éléments id, $s$, $s^2$ et $s^3$ sont deux à deux différents.

**c)** Soit $G$ la partie de $\mathscr{S}_4$ définie par $G = \{\mathrm{id}, s, s^2, s^3\}$. Montrer que $G$ est un sous-groupe de $\mathscr{S}_4$.

**17.** Soient $H$ et $G$ les deux sous-groupes de $\mathscr{S}_4$ définis par

$$H = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \quad \text{et} \quad G = \{\mathrm{id}, (1234), (13)(24), (1432)\}.$$

**a)** Supposons que $f$ est un homomorphisme de $H$ dans $G$. Montrer que pour tout $s \in H$, on a $(f(s))^2 = \mathrm{id}$.

**b)** Démontrer que les groupes $H$ et $G$ ne sont pas isomorphes.

**18.** Posons $K = \{\, s \in \mathscr{S}_4 \mid s(3) = 3 \,\}$.

**a)** Montrer que $K$ est un sous-groupe de $\mathscr{S}_4$.

**b)** Montrer que pour tout $s \in K$ et pour tout $i \in \{1, 2, 4\}$, on a $s(i) \neq 3$. En déduire que les groupes $K$ et $\mathscr{S}(\{1, 2, 4\})$ sont isomorphes.

**c)** Montrer que les groupes $K$ et $\mathscr{S}_3$ sont isomorphes.

**19. a)** Soit $s$ un élément du groupe $\mathscr{S}_4$ tel que $s(1\ 2) = (1\ 2)s$. Montrer que l'on a $\{s(3), s(4)\} = \{3, 4\}$.

**b)** Soit $s$ un élément du groupe $\mathscr{S}_4$ tel que $s(1\ 2) = (1\ 2)s$ et $s(1\ 3) = (1\ 3)s$. Montrer que $s = \mathrm{id}$.

**20.** Notons $s$ l'élément de $\mathscr{S}_9$ défini par

$$\begin{cases} s(1) = 3 & s(4) = 5 & s(7) = 1 \\ s(2) = 8 & s(5) = 9 & s(8) = 6 \\ s(3) = 7 & s(6) = 2 & s(9) = 4. \end{cases}$$

**a)** Décomposer $s$ en produit de cycles à supports disjoints.

**b)** Trouver le plus petit entier positif $n$ tel que $s^n = \mathrm{id}$.

**21.** Notons $s$ et $s'$ les éléments de $\mathscr{S}_9$ définis par

$$\begin{cases} s(1) = 2 & s(4) = 4 & s(7) = 7 \\ s(2) = 1 & s(5) = 8 & s(8) = 6 \\ s(3) = 3 & s(6) = 5 & s(9) = 9 \end{cases} \qquad \begin{cases} s'(1) = 1 & s'(4) = 3 & s'(7) = 9 \\ s'(2) = 2 & s'(5) = 5 & s'(8) = 8 \\ s'(3) = 4 & s'(6) = 6 & s'(9) = 7. \end{cases}$$

**a)** Décomposer $s$ et $s'$ en produit de cycles à supports disjoints.

**b)** Démontrer que l'on a $ss' = s's$.

**c)** Trouver le plus petit entier positif $n$ tel que $(ss')^n = \mathrm{id}$.

**22.** Soit $G$ l'ensemble des matrices de $M_2(\mathbb{R})$ de la forme $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$, où $a, b, c$ sont des nombres réels et $ac \neq 0$.

**a)** Montrer que $G$ est un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$.

**b)** Soit $H$ l'ensemble des matrices de $G$ de la forme $\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$. Montrer que $H$ est un sous-groupe de $G$ isomorphe à $\mathbb{R}$ muni de l'addition.

**c)** Déterminer les éléments $M \in G$ tels que $M \neq I_2$ et $M^2 = I_2$.

**d)** Trouver des éléments $A$ et $B$ de $G$ tels que $A^2 = B^2 = I_2$ et $(AB)^n \neq I_2$ quel que soit l'entier positif $n$.

## Quelques réponses ou indications

2. **b)** Écrire $xy = (xy)^{-1}$.

4. **b)** Ces nombres complexes ont des arguments différents.

**c)** On a $\omega^6 = 1$ donc pour tout entier naturel $n$, $\omega^n = \omega^r$ où $r$ est le reste de la division euclidienne de $n$ par 6. Si $p$ et $q$ sont des entiers compris entre 0 et 5, alors $\omega^p\omega^q = \omega^{p+q}$ appartient à $G$. De plus, on a $\omega^{-1} = \omega^5$, $(\omega^3)^{-1} = \omega^3$ et $(\omega^2)^{-1} = \omega^4$. Noter que l'on a $G = \mathbb{U}_6$.

**e)** Les nombres $\omega^2$ et $\omega^3$ ne peuvent appartenir tous les deux à $H$, sinon $\omega^3(\omega^2)^{-1} = \omega$ appartiendrait à $H$.

**f)** Montrer que si $H$ est un sous-groupe de $G$ contenant $\omega$ ou $\omega^5$, alors $H = G$. Les sous-groupes de $G$ sont $\{1\}$, $H$, $K$ et $G$.



5. Il y en a six.

6. **b)** On a $f_{a,b} \circ f_{c,d} = f_{ac,ad+b}$, $f_{1,0} = \mathrm{id}$ et si $a \neq 0$, alors $f_{a,b}^{-1} = f_{1/a,-b/a}$. On a par exemple $f_{1,1} \circ f_{-1,0} \neq f_{-1,0} \circ f_{1,1}$, donc le groupe $G$ n'est pas commutatif.

10. **a)** Pour tout nombre complexe $z$ et pour tout entier $q$, on a $z^{qd} = (z^d)^q$.

**c)** Pour montrer que l'application $f$ est surjective, remarquer que tout nombre complexe possède au moins une racine $k$-ième.

11. **a)** Utiliser l'égalité $x + y - xy - 1 = (x-1)(1-y)$.

**b)** L'élément neutre est 0 et si $x \in \mathbb{R} \setminus \{1\}$, le symétrique de $x$ est $x/(x-1)$.

14. **a)** L'application $s$ est bijective et $i$ est différent de $j$.

**b)** On a $st(s^{-1})(s(i)) = st(i) = s(j)$. Soit $k \in \{1, 2, \ldots, n\}$. Il existe $\ell \in \{1, 2, \ldots, n\}$ tel que $k = s(\ell)$. Si $k \neq s(i)$ et $k \neq s(j)$, alors on a $\ell \neq i$ et $\ell \neq j$.

15. **c)** Supposons par exemple $t = (1\ 2)(3\ 4)$ ; alors on a

$$st(s^{-1}) = s(1\ 2)(3\ 4)(s^{-1}) = \big(s(1\ 2)(s^{-1})\big)\big(s(3\ 4)(s^{-1})\big).$$

Utiliser l'exercice précédent pour calculer $st(s^{-1})$.

16. **a)** On a $s^2 = (1\ 3)(2\ 4)$ et $s^3 = (1\ 4\ 3\ 2)$.

17. **b)** Supposons que $f$ est un homomorphisme de $H$ dans $G$. Puisque $(1\ 2\ 3\ 4)^2 \neq \mathrm{id}$, alors d'après (a) on a $f(s) \neq (1\ 2\ 3\ 4)$ pour tout $s \in H$.

18. **b)** Si $s \in K$, on définit une bijection de $\{1, 2, 4\}$ dans lui-même en posant $u(1) = s(1)$, $u(2) = s(2)$ et $u(4) = s(4)$. Alors l'application de $K$ dans $\mathscr{S}(\{1, 2, 4\})$ qui à $s$ associe $u$ est un isomorphisme de groupes.

**c)** Utiliser l'exercice du paragraphe 3 pour démontrer que le groupe $\mathscr{S}(\{1, 2, 4\})$ est isomorphe à $\mathscr{S}_3$.

20. **a)** On trouve $s = (1\ 3\ 7)(2\ 8\ 6)(4\ 5\ 9)$.

**b)** La réponse est $n = 3$.

22. **c)** Ce sont les matrices de la forme $\begin{bmatrix} 1 & b \\ 0 & -1 \end{bmatrix}$ ou bien $\begin{bmatrix} -1 & b \\ 0 & 1 \end{bmatrix}$, ainsi que la matrice $-I_2$.

**d)** Par exemple, les matrices $A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ et $B = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}$ conviennent.

# Chapitre 12

# Anneaux et corps

## 1. Définitions et règles de calcul

Soit $A$ un ensemble non vide muni de deux opérations, la somme et le produit. Pour tous $x, y \in A$, la somme de $x$ et $y$ se note $x+y$ et le produit de $x$ par $y$ se note $xy$.

**Définition**

On dit que $A$ est un *anneau* si les conditions suivantes sont réalisées :

- muni de l'opération somme, $A$ est un groupe commutatif
- pour tous $x, y, z \in A$, on a $x(yz) = (xy)z$ et cet élément est noté $xyz$
- il existe $e \in A$ tel que $ex = xe = x$ pour tout $x \in A$
- pour tous $x, y, z \in A$, on a $x(y+z) = xy + xz$ et $(x+y)z = xz + yz$.

Jusqu'à la fin de ce paragraphe, supposons que $A$ est un anneau.

Par analogie avec le calcul sur les nombres et avec le calcul dans un groupe $G$ général, nous allons adopter un certain nombre de conventions d'écriture.

L'élément neutre de $A$ pour l'opération somme est noté 0, le symétrique de $x$ est noté $-x$ et s'appelle l'*opposé* de $x$. De plus, la somme de $x$ et $-y$ se note $x-y$.

Comme dans le cas d'un groupe, l'élément $e$ est nécessairement unique. On l'appelle l'élément neutre de $A$ pour l'opération produit et on convient de le noter 1 en général.

Soit $x \in A$. S'il existe $x' \in A$ tel que $xx' = x'x = 1$, alors cet élément $x'$ est unique et s'appelle le symétrique de $x$ pour l'opération produit. En effet, si l'on a $xx' = x'x = 1$ et $xx'' = x''x = 1$, il vient $x' = x'1 = x'(xx'') = (x'x)x'' = 1x'' = x''$.

**Lemme.** *Pour tout $x \in A$, on a $0x = 0$ et $(-1)x = -x$.*

**Démonstration.** Soit $x \in A$. Il vient $0x = (0+0)x = 0x + 0x$, d'après les règles de calcul. Puisque l'ensemble $A$ muni de l'addition est un groupe, nous pouvons

simplifier cette égalité par $0x$. On obtient ainsi $0x = 0$.
Puisque $1x = x$, nous avons $x + (-1)x = 1x + (-1)x = (1 + (-1))x = 0x$, donc $x + (-1)x = 0$. Il s'ensuit que le produit $(-1)x$ est l'opposé de $x$. ∎

**Définition**
Si l'on a $xy = yx$ pour tous $x, y \in G$, on dit que $A$ est un anneau *commutatif*.

**Exemples**

1) Les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des anneaux commutatifs.
2) Si $\mathbf{K} = \mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, alors $\mathbf{K}[X]$ est un anneau commutatif.
3) Si $\mathbf{K} = \mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ et si $n$ est un entier supérieur ou égal à 2, alors $M_n(\mathbf{K})$ est un anneau non commutatif. Le produit de deux matrices est le produit défini au chapitre 4. L'élément neutre de $M_n(\mathbf{K})$ pour le produit est la matrice $I_n$.

**Notation.** Soit $x \in A$. Posons $x^0 = 1$ et pour tout entier positif $n$, notons $x^n$ le produit de $x^{n-1}$ par $x$. Pour tous entiers naturels $n$ et $k$, on a

$$x^n x^k = x^{n+k} \quad \text{et} \quad (x^n)^k = x^{nk}.$$

Nous avons vu que la formule du binôme de Newton est vraie dans $\mathbb{C}$ et dans $\mathbf{K}[X]$. En voici sa généralisation.

**Formule du binôme de Newton.** Soient $x$ et $y$ des éléments de $A$. Si $xy = yx$, alors pour tout entier $p$ supérieur ou égal à 2, on a

$$(x+y)^p = x^p + C_p^1 x^{p-1}y + \cdots + C_p^k x^{p-k}y^k + \cdots + C_p^{p-1}xy^{p-1} + y^p.$$

**Remarque**
L'anneau $M_n(\mathbf{K})$ n'étant pas commutatif, si $X$ et $Y$ sont des matrices, l'hypothèse $XY = YX$ est indispensable pour développer $(X+Y)^p$ selon la formule du binôme de Newton. Par exemple, puisqu'on a $I_n X = X I_n$ pour tout $X \in M_n(\mathbf{K})$, il vient $(I_n + X)^p = I_n + pX + \cdots + C_p^k X^k + \cdots + pX^{p-1} + X^p$ pour tout entier $p \geqslant 2$.

**Définition**
Soit $x \in A$. Si pour l'opération produit, l'élément $x$ a un symétrique, ce symétrique se note $x^{-1}$ et s'appelle l'*inverse* de $x$. Dans ce cas, on dit que $x$ est *inversible*.

**Proposition.** *Soient $x$ et $y$ des éléments de $A$.*
- *Si $x$ est inversible, alors $x^{-1}$ est inversible et l'on a $(x^{-1})^{-1} = x$.*
- *Si $x$ et $y$ sont inversibles, alors le produit $xy$ est inversible et l'on a $(xy)^{-1} = y^{-1}x^{-1}$.*



**Démonstration.** Supposons $x$ inversible. On a $xx^{-1} = x^{-1}x = 1$, donc par définition d'un élément inversible, on en déduit que $x^{-1}$ est inversible, d'inverse $x$. De plus, si $y$ est inversible, il vient $(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = x1x^{-1} = xx^{-1} = 1$ et $(y^{-1}x^{-1})(xy) = y^{-1}1y = y^{-1}y = 1$. Il s'ensuit que $xy$ est inversible, d'inverse $y^{-1}x^{-1}$. ∎

Notons $A^*$ l'ensemble des éléments inversibles de $A$. On a $1 \in A^*$.

Puisque le produit de deux éléments inversibles est inversible, le produit dans $A$ définit une opération dans $A^*$. Muni de cette opération, $A^*$ est un groupe : c'est ce qu'affirme la proposition suivante.

**Proposition.** *Muni de l'opération produit, $A^*$ est un groupe.*

**Démonstration.** On a $1 \in A^*$ donc $A^*$ n'est pas vide. D'après les règles de calcul dans $A$, on a $x(yz) = (xy)z$ pour tous $x, y, z \in A^*$ et $1x = x1 = x$ pour tout $x \in A^*$. Si $x \in A^*$, alors $x^{-1} \in A^*$ et $xx^{-1} = x^{-1}x = 1$. Il s'ensuit que $A^*$ est un groupe. ∎

**Exemples**

1) Le groupe des éléments inversibles de l'anneau $\mathbb{Z}$ est $\{-1, 1\}$.
2) Si $\mathbf{K} = \mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, un élément est inversible dans l'anneau $\mathbf{K}$ si et seulement s'il est différent de 0, par suite $\mathbf{K}^* = \mathbf{K} \setminus \{0\}$.
3) Si $\mathbf{K} = \mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, les éléments inversibles de l'anneau $\mathbf{K}[X]$ sont les polynômes constants non nuls. Autrement dit, on a $(\mathbf{K}[X])^* = \mathbf{K}^*$. En effet, si $P$ et $Q$ sont des polynômes tels que $PQ=1$, alors $P$ et $Q$ sont non nuls et de degré 0, donc constants.
4) Supposons $\mathbf{K} = \mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$. Soit $n$ un entier supérieur ou égal à 2. Au chapitre 4, nous avons défini ce qu'est une matrice inversible : la matrice $X \in M_n(\mathbf{K})$ est inversible s'il existe une matrice $Y \in M_n(\mathbf{K})$ telle que $XY = YX = I_n$. Une matrice de $M_n(\mathbf{K})$ est donc inversible si c'est un élément inversible de l'anneau $M_n(\mathbf{K})$. Nous avons défini au chapitre précédent (page 248) le groupe $\mathrm{GL}_n(\mathbf{K})$ des matrices inversibles de $M_n(\mathbf{K})$. On a donc $(M_n(\mathbf{K}))^* = \mathrm{GL}_n(\mathbf{K})$.

**Définition**
Soit $K$ un anneau. On dit que $K$ est un *corps* si $K$ est un anneau commutatif et si $K^*$ est égal à $K \setminus \{0\}$.

Un corps est donc un anneau commutatif dans lequel tout élément différent de 0 a un inverse pour l'opération produit. Les ensembles $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps.

## 2. Sous-anneaux et sous-corps

**Définition**
Soient $A$ un anneau et $B$ une partie de $A$. On dit que $B$ est un *sous-anneau* de $A$ si les conditions suivantes sont réalisées :
- muni de l'opération somme, $B$ est un sous-groupe de $A$
- $1 \in B$ et pour tous $x, y$ appartenant à $B$, on a $xy \in B$.

Comme dans le cas des groupes, nous avons la proposition suivante.

**Proposition.** *Soit $A$ un anneau. Si $B$ est un sous-anneau de $A$, alors muni des mêmes opérations que $A$, $B$ est un anneau.*

Ainsi, l'anneau $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$. Donnons un exemple de sous-anneau de $\mathbb{R}$, autre que $\mathbb{Z}$ ou $\mathbb{Q}$.

**Exemple.** Notons $\mathbb{Z}[\sqrt{2}]$ l'ensemble des nombres réels qui s'écrivent $a + b\sqrt{2}$, où $a, b$ sont des entiers relatifs et démontrons que $\mathbb{Z}[\sqrt{2}]$ est un sous-anneau de $\mathbb{R}$.
On a $0 = 0 + 0\sqrt{2}$ et $1 = 1 + 0\sqrt{2}$, par suite $0 \in \mathbb{Z}[\sqrt{2}]$ et $1 \in \mathbb{Z}[\sqrt{2}]$.
D'après les règles de calcul dans $\mathbb{R}$, on a pour tous $a, b, c, d \in \mathbb{Z}$,

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}, \quad -(a + b\sqrt{2}) = (-a) + (-b)\sqrt{2}$$

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}.$$

Puisque $ac + 2bd$ et $ad + bc$ sont des entiers, il s'ensuit que pour tous $x, y \in \mathbb{Z}[\sqrt{2}]$, on a $x + y \in \mathbb{Z}[\sqrt{2}]$, $-x \in \mathbb{Z}[\sqrt{2}]$ et $xy \in \mathbb{Z}[\sqrt{2}]$. On a donc démontré que $\mathbb{Z}[\sqrt{2}]$ est un sous-anneau de $\mathbb{R}$.

**Définition**
Soient $K$ un corps et $L$ une partie de $K$. On dit que $L$ est un *sous-corps* de $K$ si $L$ est un sous-anneau de $K$ et si pour tout $x \in L \setminus \{0\}$, on a $x^{-1} \in L$.

**Proposition.** *Soit $K$ un corps. Si $L$ est un sous-corps de $K$, alors muni des mêmes opérations que $K$, $L$ est un corps.*

Ainsi le corps $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$, qui est lui-même un sous-corps de $\mathbb{C}$. Voici un exemple de sous-corps de $\mathbb{C}$ qui n'est pas contenu dans $\mathbb{R}$ et qui est différent de $\mathbb{C}$.

**Exemple.** Notons $\mathbb{Q}(i)$ l'ensemble des nombres complexes qui s'écrivent $a + bi$ où $a, b$ sont des nombres rationnels et démontrons que $\mathbb{Q}(i)$ est un sous-corps de $\mathbb{C}$.



D'après les règles de calcul dans $\mathbb{C}$, on a pour tous $a, b, c, d \in \mathbb{Q}$,
$(a + bi) + (c + di) = (a + c) + (b + d)i$ et $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$.
De plus, si $a$ et $b$ sont des nombres rationnels non tous deux nuls, on a

$$\frac{1}{a + bi} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i$$

et les nombres $a/(a^2 + b^2)$ et $-b/(a^2 + b^2)$ sont rationnels. Il s'ensuit que $\mathbb{Q}(i)$ est un sous-corps de $\mathbb{C}$. On a $i \in \mathbb{Q}(i)$, donc $\mathbb{Q}(i)$ n'est pas contenu dans $\mathbb{R}$. Puisque $\sqrt{2} \notin \mathbb{Q}$, on a $\sqrt{2} \notin \mathbb{Q}(i)$ et donc $\mathbb{Q}(i)$ est différent de $\mathbb{C}$.

## 3. Le corps des fractions rationnelles

Dans ce paragraphe, $\mathbb{K}$ est le corps $\mathbb{R}$ ou le corps $\mathbb{C}$ et les polynômes considérés sont à coefficients dans $\mathbb{K}$.
Une *fraction rationnelle* s'écrit $\frac{A}{B}$ où $A$ et $B$ sont des polynômes et où $B \neq 0$. De plus, on convient que l'on a $\frac{A}{B} = \frac{C}{D}$ si et seulement si on a l'égalité $AD = BC$ dans l'anneau des polynômes $\mathbb{K}[X]$. En particulier, si $P$ est un polynôme non nul, on a $\frac{PA}{PB} = \frac{A}{B}$.
L'ensemble des fractions rationnelles à coefficients dans $\mathbb{K}$ se note $\mathbb{K}(X)$.

**Exemples**
- La fraction rationnelle $\frac{X^3 + X^2 + X + 1}{X^4 + X^3 + X + 1}$ est à coefficients réels. Puisqu'on a $X^3 + X^2 + X + 1 = (X + 1)(X^2 + 1)$ et $X^4 + X^3 + X + 1 = (X + 1)(X^3 + 1)$, il s'ensuit $\frac{X^3 + X^2 + X + 1}{X^4 + X^3 + X + 1} = \frac{X^2 + 1}{X^3 + 1}$.
- La fraction rationnelle $\frac{X}{X^2 + i}$ est à coefficients complexes.

On définit les opérations somme et produit dans $\mathbb{K}(X)$ de la manière suivante :

$$\frac{A}{B} + \frac{C}{D} = \frac{AD + BC}{BD} \quad \text{et} \quad \frac{A}{B}\frac{C}{D} = \frac{AD}{BD}.$$

Il faut bien entendu vérifier que ces définitions ont un sens, autrement dit que faire la somme ou le produit de deux fractions rationnelles ne dépend que des fractions rationnelles $\frac{A}{B}$ et $\frac{C}{D}$ et non des choix possibles des polynômes $A, B, C, D$. Il s'agit de démontrer que si dans l'anneau des polynômes $\mathbb{K}[X]$, on a $A_1B_2 = A_2B_1$ et $C_1D_2 = C_2D_1$, cela entraîne les égalités

$$(A_1D_1 + B_1C_1)B_2D_2 = (A_2D_2 + B_2C_2)B_1D_1 \quad \text{et} \quad (A_1C_1)(B_2D_2) = (A_2C_2)(B_1D_1).$$

Et cette affirmation se vérifie en appliquant les règles de calcul dans l'anneau des polynômes $\mathbb{K}[X]$.

### Valeur d'une fraction rationnelle

Si $\frac{A}{B}$ est une fraction rationnelle et si $x \in \mathbb{C}$ n'est pas racine de $B$, la valeur de $\frac{A}{B}$ en $x$ est le nombre complexe $\frac{A}{B}(x) = \frac{A(x)}{B(x)}$. Cela a un sens, car si $\frac{A}{B} = \frac{C}{D}$ et si $x$ n'est pas racine de $D$, alors on a $\frac{A(x)}{B(x)} = \frac{C(x)}{D(x)}$. D'après les propriétés des fonctions polynôme, si $x \in \mathbb{C}$ n'est racine ni de $B$, ni de $D$, on a

$$\left(\frac{A}{B} + \frac{C}{D}\right)(x) = \frac{A(x)}{B(x)} + \frac{C(x)}{D(x)} \quad \text{et} \quad \left(\frac{A}{B}\,\frac{C}{D}\right)(x) = \frac{A(x)\,C(x)}{B(x)\,D(x)}.$$

**Convention.** Puisque dans $\mathbb{K}(X)$, le calcul sur les fractions rationnelles de la forme $\frac{P}{1}$ est le même que celui sur les polynômes $P$, on convient de poser $\frac{P}{1} = P$. Ainsi on a $\mathbb{K}[X] \subset \mathbb{K}(X)$.

Par exemple, dans $\mathbb{C}(X)$, on a $\frac{X^4+1}{X^2+i} = \frac{X^2-i}{1} = X^2 - i$.

### Remarque importante

Les règles de calcul sur les fractions rationnelles sont exactement les mêmes que celles sur les nombres rationnels.

**Proposition.** *Muni de la somme et du produit,* $\mathbb{K}(X)$ *est un corps.*

Indiquons juste que l'opposé de $\frac{A}{B}$ est $\frac{-A}{B}$ et que si $A$ et $B$ sont des polynômes non nuls, l'inverse de $\frac{A}{B}$ est la fraction rationnelle $\frac{B}{A}$.

**Proposition.** *Si* $\frac{A}{B}$ *est une fraction rationnelle, alors il existe un unique polynôme* $Q$*, appelé* partie entière *de* $\frac{A}{B}$*, tel que* $\frac{A}{B} = Q + \frac{R}{B}$*, où* $R$ *est un polynôme vérifiant* $R = 0$ *ou* $\deg R < \deg B$.

**Démonstration.** Puisque le polynôme $B$ n'est pas nul, on a $\frac{A}{B} = Q + \frac{R}{B}$ dans le corps $\mathbb{K}(X)$, si et seulement si on a $A = BQ + R$ dans l'anneau $\mathbb{K}[X]$. Notons $Q_1$ le quotient de la division euclidienne de $A$ par $B$ : $Q_1$ est l'unique polynôme de $\mathbb{K}[X]$ tel que $A - BQ_1 = 0$ ou $\deg(A - BQ_1) < \deg B$. Le polynôme $Q_1$ répond donc à la question.





Pour démontrer l'unicité, il s'agit de prouver que si $\frac{A}{B} = \frac{C}{D}$, c'est-à-dire si $AD = BC$, alors le quotient de la division euclidienne de $C$ par $D$ est égal à $Q_1$. Puisque le polynôme $D$ n'est pas nul, $Q_1$ est le quotient de la division euclidienne de $AD$ par $BD$. En effet, on a $AD - BDQ_1 = D(A - BQ_1)$ et $D(A - BQ_1) = 0$ ou bien $\deg(D(A - BQ_1)) = \deg D + \deg(A - BQ_1) < \deg D + \deg B = \deg(DB)$.

Notons $Q_2$ le quotient de la division euclidienne de $C$ par $D$. Puisque le polynôme $B$ n'est pas nul, on en déduit comme précédemment que $Q_2$ est le quotient de la division euclidienne de $BC$ par $BD$. Enfin, puisqu'on a $AD = BC$ et par unicité du quotient de la division euclidienne de $AD$ par $BD$, on en déduit $Q_1 = Q_2$. ∎

> La partie entière de $\frac{A}{B}$ est le quotient de la division euclidienne de $A$ par $B$.

Intéressons-nous maintenant aux fractions rationnelles de partie entière nulle. Commençons par définir certaines fractions rationnelles particulières.

### Élément simple de $\mathbb{C}(X)$

C'est par définition une fraction rationnelle de la forme $\frac{a}{(X-b)^n}$ où $a \in \mathbb{C}^*$, $b \in \mathbb{C}$ et où $n$ est un entier positif.

### Élément simple de $\mathbb{R}(X)$

Par définition, c'est une fraction rationnelle de l'une des formes suivantes :

- $\frac{a}{(X-b)^n}$ où $a \in \mathbb{R}^*$, $b \in \mathbb{R}$ et où $n$ est un entier positif
- $\frac{aX+b}{(X^2+pX+q)^n}$, où $a$ et $b$ sont des nombres réels non tous deux nuls, où $p$ et $q$ sont des nombres réels tels que $p^2 - 4q < 0$ et où $n$ est un entier positif.

### Exemples

- La fraction rationnelle $\frac{1}{(X-i)^3}$ est un élément simple de $\mathbb{C}(X)$.
- La fraction rationnelle $\frac{2X+3}{X^2+X+1}$ est un élément simple de $\mathbb{R}(X)$, mais n'est pas un élément simple de $\mathbb{C}(X)$.

**Théorème.** *Si* $A$ *et* $B$ *sont des polynômes non nuls de* $\mathbb{K}[X]$ *tels que* $\deg A < \deg B$*, alors la fraction rationnelle* $\frac{A}{B}$ *s'écrit de manière unique comme somme d'éléments simples de* $\mathbb{K}(X)$.

Nous n'allons pas démontrer ce théorème, mais nous allons apprendre à le pratiquer sur des exemples où les calculs ne sont pas trop compliqués. Cela est notamment utile en analyse pour trouver une primitive d'une fonction rationnelle.

Si $\frac{A}{B}$ est une fraction rationnelle non nulle de $\mathbb{K}(X)$, on peut trouver l'unique polynôme $Q \in \mathbb{K}[X]$ tel que $\frac{A}{B} = Q + \frac{R}{B}$. Dans le cas où $R \neq 0$, *décomposer* $\frac{A}{B}$ *en éléments simples* sur $\mathbb{K}$, c'est trouver $Q$ et les éléments simples de somme $\frac{R}{B}$.

### Format de la décomposition en éléments simples

Soit $\frac{A}{B}$ une fraction rationnelle de $\mathbb{K}(X)$, qui n'est pas un polynôme. Supposons les polynômes $A$ et $B$ premiers entre eux. Les éléments simples qui apparaissent dans la décomposition de $\frac{A}{B}$ ont pour dénominateur un polynôme de la forme $P^k$, où $P \in \mathbb{K}[X]$ est un facteur irréductible de $B$ et où $k$ est un entier compris entre 1 et $n$, $P^n$ étant la plus grande puissance de $P$ qui divise $B$.

### Exemples de format

1) Considérons la fraction rationnelle $\frac{X^2+X+1}{(X^2+1)^2(X-1)^2}$. Le degré du numérateur est plus petit que celui du dénominateur, donc la partie entière est nulle. Le format de la décomposition en éléments simples sur $\mathbb{R}$ de cette fraction rationnelle est ainsi

$$\frac{X^2+X+1}{(X^2+1)^2(X-1)^2} = \frac{aX+b}{(X^2+1)^2} + \frac{cX+d}{X^2+1} + \frac{e}{(X-1)^2} + \frac{f}{X-1}$$

où $a, b, c, d, e, f$ sont des nombres réels.

2) Le format de la décomposition en éléments simples sur $\mathbb{C}$ de la même fraction rationnelle est

$$\frac{X^2+X+1}{(X^2+1)^2(X-1)^2} = \frac{p}{(X-i)^2} + \frac{q}{X-i} + \frac{r}{(X+i)^2} + \frac{s}{X+i} + \frac{t}{(X-1)^2} + \frac{u}{X-1}$$

où $p, q, r, s, t, u$ sont des nombres complexes.

3) La partie entière de la fraction rationnelle $\frac{X^3+2}{(X-1)^2(X+1)}$ étant égale à 1, le format de sa décomposition en éléments simples sur $\mathbb{R}$ est

$$\frac{X^3+2}{(X-1)^2(X+1)} = 1 + \frac{a}{(X-1)^2} + \frac{b}{X-1} + \frac{c}{X+1}$$

où $a, b, c$ sont des nombres réels.





Lorsqu'on décompose une fraction rationnelle en éléments simples, on doit dans un premier temps trouver la partie entière de cette fraction, et dans un deuxième temps écrire le format de la décomposition.

Voici maintenant quelques exemples où l'on peut aisément calculer les numérateurs des éléments simples qui apparaissent dans la décomposition.

**Exemple 1.** Décomposons en éléments simples sur $\mathbb{R}$ la fraction rationnelle $\frac{X^3+1}{(X-1)^4}$. La partie entière de cette fraction rationnelle est nulle. D'autre part, on sait (voir chapitre 10) que $\left((X-1)^3, (X-1)^2, X-1, 1\right)$ est une base de l'espace vectoriel des polynômes de $\mathbb{R}[X]$ nul ou de degré inférieur ou égal à 3. Cherchons les coordonnées du polynôme $X^3+1$ dans cette base. On a

$$X^3+1 = \left((X-1)+1\right)^3 + 1 = (X-1)^3 + 3(X-1)^2 + 3(X-1) + 2.$$

On en déduit la décomposition en éléments simples sur $\mathbb{R}$ suivante :

$$\frac{X^3+1}{(X-1)^4} = \frac{2}{(X-1)^4} + \frac{3}{(X-1)^3} + \frac{3}{(X-1)^2} + \frac{1}{X-1}.$$

**Exemple 2.** Décomposons en éléments simples sur $\mathbb{R}$ la fraction rationnelle $\frac{3}{X^3+1}$. Factorisons $X^3+1$ en produit de polynômes irréductibles de $\mathbb{R}[X]$. Puisque $-1$ est racine de $X^3+1$, le polynôme $X^3+1$ est divisible par $X+1$. Précisément, on a $X^3+1 = (X+1)(X^2-X+1)$. Le polynôme $X^2-X+1$ a un discriminant strictement négatif, donc c'est un polynôme irréductible de $\mathbb{R}[X]$. De plus, on a la division euclidienne $X^2-X+1 = (X+1)(X-2)+3$. On en déduit $3 = (X^2-X+1)+(X+1)(2-X)$. La décomposition en éléments simples sur $\mathbb{R}$ de la fraction rationnelle $\frac{3}{X^3+1}$ est donc

$$\frac{3}{X^3+1} = \frac{1}{X+1} + \frac{2-X}{X^2-X+1}.$$

**Exemple 3.** Décomposons en éléments simples sur $\mathbb{R}$, la fraction rationnelle $\frac{X^4+1}{(X-1)^2(X^2+1)}$. Le numérateur et le dénominateur de cette fraction rationnelle n'ont aucune racine commune dans $\mathbb{C}$, par suite ce sont des polynômes premiers entre eux. D'autre part, le numérateur et le dénominateur sont unitaires et ont même degré, donc la partie entière est égale à 1. Le format de la décomposition en éléments simples sur $\mathbb{R}$ est donc

$$\frac{X^4+1}{(X-1)^2(X^2+1)} = 1 + \frac{a}{(X-1)^2} + \frac{b}{X-1} + \frac{cX+d}{X^2+1}$$

où $a, b, c, d$ sont des nombres réels.

– ***Calcul de a.*** Dans le corps $\mathbb{R}(X)$, multiplions la fraction rationnelle ci-dessus par le polynôme $(X-1)^2$. On obtient

$$\frac{X^4+1}{X^2+1} = (X-1)^2 + a + b(X-1) + \frac{(cX+d)(X-1)^2}{X^2+1}.$$

Prenons alors la valeur de cette nouvelle fraction rationnelle en $1$ : il vient $\frac{1+1}{1+1} = a$, par suite $a = 1$. On en déduit

$$\frac{X^4+1}{(X-1)^2(X^2+1)} = 1 + \frac{1}{(X-1)^2} + \frac{b}{X-1} + \frac{cX+d}{X^2+1}.$$

– ***Calcul de c et d.*** Dans le corps $\mathbb{R}(X)$, multiplions la fraction rationnelle ci-dessus par le polynôme $X^2+1$. Nous avons

$$\frac{X^4+1}{(X-1)^2} = X^2+1+\frac{X^2+1}{(X-1)^2} + \frac{b(X^2+1)}{X-1} + cX + d.$$

Prenons la valeur de cette fraction rationnelle en $i$. Il vient $\frac{i^4+1}{(i-1)^2} = ci+d$. Or on a $(i-1)^2 = i^2-2i+1 = -2i$ et $i^4+1 = 2$. On en déduit $i = ci+d$, d'où $c = 1$ et $d = 0$. On a ainsi l'égalité

$$\frac{X^4+1}{(X-1)^2(X^2+1)} = 1 + \frac{1}{(X-1)^2} + \frac{b}{X-1} + \frac{X}{X^2+1}.$$

– ***Calcul de b.*** Prenons la valeur en 0 de cette fraction rationnelle. Il vient $1 = 1+1-b$, d'où $b = 1$. La décomposition en éléments simples sur $\mathbb{R}$ de la fraction rationnelle $\frac{X^4+1}{(X-1)^2(X^2+1)}$ est donc

$$\frac{X^4+1}{(X-1)^2(X^2+1)} = 1 + \frac{1}{(X-1)^2} + \frac{1}{X-1} + \frac{X}{X^2+1}.$$

**Exemple 4.** Décomposons en éléments simples sur $\mathbb{C}$ la fraction rationnelle $\frac{X^4+1}{(X+i)(X^2-2i)}$. Factorisons le polynôme $X^2-2i$. Il s'agit de trouver les racines carrées du nombre complexe $2i$. La méthode a été expliquée au chapitre 3, page 39. Ici on trouve $(1+i)^2 = 2i$, d'où la factorisation $X^2-2i = (X-1-i)(X+1+i)$. Puisque ni $-i$, ni $1+i$, ni $-1-i$ ne sont racines de $X^4+1$, les polynômes $X^4+1$ et $(X+i)(X^2-2i)$ sont premiers entre eux. Calculons maintenant la partie entière de la fraction rationnelle $\frac{X^4+1}{(X+i)(X^2-2i)}$. On a $(X+i)(X^2-2i) = X^3+iX^2-2iX+2$ et la division euclidienne

$$X^4+1 = (X^3+iX^2-2iX+2)(X-i) + (2i-1)X^2+1+2i,$$





par suite la partie entière est égale à $X-i$. Voici donc le format de la décomposition en éléments simples, où $a, b, c$ sont des nombres complexes :

$$\frac{X^4+1}{(X+i)(X-1-i)(X+1+i)} = X - i + \frac{a}{X+i} + \frac{b}{X+1+i} + \frac{c}{X-1-i}.$$

Pour calculer $a$, multiplions la fraction rationnelle ci-dessus par le polynôme $X+i$. On obtient dans le corps $\mathbb{C}(X)$ l'égalité

$$\frac{X^4+1}{X^2-2i} = (X-i)(X+i) + a + \frac{b(X+i)}{X+1+i} + \frac{c(X+i)}{X-1-i}.$$

En prenant la valeur en $-i$, on trouve $a = \frac{i^4+1}{i^2-2i} = \frac{-2}{1+2i} = \frac{-2+4i}{5}$.

Pour calculer $b$, on multiplie la fraction rationnelle par $X+1+i$, puis on prend la valeur en $-1-i$. On obtient $b = \frac{(1+i)^4+1}{(-1-i+i)(-2-2i)} = \frac{-3}{2(1+i)} = \frac{-3+3i}{4}$.

Pour calculer $c$, on multiplie la fraction rationnelle par $X-1-i$ et l'on prend la valeur en $1+i$, ce qui donne $c = \frac{(1+i)^4+1}{(1+i+i)(2+2i)} = \frac{-3}{2(-1+3i)} = \frac{3+9i}{20}$.

La décomposition en éléments simples sur $\mathbb{C}$ cherchée est donc

$$\frac{X^4+1}{(X+i)(X^2-2i)} = X - i + \frac{-2+4i}{5(X+i)} + \frac{-3+3i}{4(X+1+i)} + \frac{3+9i}{20(X-1-i)}.$$

Donnons pour finir une méthode de calcul pour décomposer une fraction rationnelle en éléments simples, lorsque le dénominateur est de la forme $(X-a)^nV$, où $V$ est un polynôme non constant tel que $V(a) \neq 0$ et où $n$ est un entier supérieur ou égal à 2. Pour cela, nous avons besoin d'énoncer un résultat sur les polynômes.

**Proposition.** *Soient $A, B$ des polynômes et soit $n$ un entier naturel. Si 0 n'est pas racine de $B$, alors il existe un unique polynôme $Q$ nul ou de degré inférieur ou égal à $n$, tel que $A - BQ$ est divisible par $X^{n+1}$.*

**Démonstration abrégée.** L'existence d'un tel polynôme se démontre par récurrence sur l'entier $n$. Démontrons l'unicité. Supposons qu'il existe *a priori* deux polynômes $Q_1$ et $Q_2$ comme dans la proposition. Le polynôme $(A-BQ_1)-(A-BQ_2) = B(Q_2-Q_1)$ est alors divisible par $X^{n+1}$. Puisque 0 n'est pas racine de $B$, les polynômes $X^{n+1}$ et $B$ sont premiers entre eux. D'après le théorème de Gauss (page 229), il s'ensuit que $X^{n+1}$ divise $Q_2-Q_1$. Mais le polynôme $Q_2-Q_1$ est nul ou de degré inférieur ou égal à $n$, par suite $Q_2-Q_1=0$, c'est-à-dire $Q_2=Q_1$. ∎

Dans la proposition, le polynôme $Q$ s'appelle le *quotient à l'ordre $n$ de la division de $A$ par $B$ selon les puissances croissantes.*

**Remarque utile**

Notons $T_n(A)$ le polynôme obtenu à partir de $A$ en supprimant les termes de degré strictement plus grand que $n$. Par exemple, $T_2\big((X+1)^4\big) = 6X^2+4X+1$. Alors le quotient à l'ordre $n$ de la division de $A$ par $B$ selon les puissances croissantes est égal au quotient à l'ordre $n$ de la division de $T_n(A)$ par $B$ selon les puissances croissantes.

Voyons sur un exemple comment on pratique cette proposition pour décomposer en éléments simples une fraction rationnelle.

**Exemple 5.** Décomposons la fraction rationnelle $\dfrac{X^4+1}{(X-1)^3(X-2)}$ en éléments simples sur $\mathbb{R}$. Le numérateur et le dénominateur sont des polynômes de même degré, unitaires et premiers entre eux. Voici donc le format de la décomposition en éléments simples sur $\mathbb{R}$, où $a, b, c, d$, sont des nombres réels :

$$\frac{X^4+1}{(X-1)^3(X-2)} = 1 + \frac{a}{(X-1)^3} + \frac{b}{(X-1)^2} + \frac{c}{X-1} + \frac{d}{X-2}.$$

Posons $U = X^4+1$ et $V = X-2$ et considérons les polynômes composés (voir page 222)

$$A = U\circ(X+1) = (X+1)^4+1 \quad \text{et} \quad B = V\circ(X+1) = (X+1)-2 = X-1.$$

Notons $Q$ le quotient à l'ordre 2 de la division de $A$ par $B$ selon les puissances croissantes : on a $A - BQ = X^3S$, où $S \in \mathbb{R}[X]$. Dans le corps $\mathbb{R}(X)$, il vient

$$\frac{A}{X^3B} = 1 + \frac{a}{X^3} + \frac{b}{X^2} + \frac{c}{X} + \frac{d}{X-1} \quad \text{et} \quad \frac{A}{X^3B} = \frac{Q}{X^3} + \frac{S}{B}.$$

Par unicité de la décomposition en éléments simples et d'après le format de la décomposition en éléments simples de $\dfrac{S}{B}$, il s'ensuit $Q = a + bX + cX^2$. D'après la remarque, $Q$ est le quotient à l'ordre 2 de la division de $T_2(A)$ par $B$ selon les puissances croissantes. Or on a

$$T_2(A) = T_2(X^4+4X^3+6X^2+4X+2) = 6X^2+4X+2.$$

Pour calculer le polynôme $Q$, on commence par écrire les polynômes $T_2(A)$ et $B$ dans l'ordre croissant des puissances de $X$ : on a

$$T_2(A) = 2+4X+6X^2 \quad \text{et} \quad B = -1+X.$$

Pour diviser $2+4X+6X^2$ par $-1+X$, on commence par diviser 2 par $-1$ : on trouve $-2$. On écrit alors

$$2+4X+6X^2 = -2(-1+X)+6X+6X^2.$$





On continue en divisant le polynôme $6X+6X^2$ par $-1+X$ en utilisant la même méthode : le quotient de $6X$ par $-1$ est $-6X$ donc on obtient

$$6X+6X^2 = -6X(-1+X)+12X^2.$$

Enfin, on a $12X^2 = -12X^2(-1+X)+12X^3$. Il s'ensuit

$$T_2(A) = (-2-6X-12X^2)B + 12X^3, \quad \text{donc} \quad Q = -2-6X-12X^2.$$

Une manière de disposer les calculs que nous venons de faire est la suivante.

$$\begin{array}{rr|l}
 & 2+4X+6X^2 & -1+X \\
- & 2-2X & -2-6X-12X^2 \\ \hline
 & 6X+6X^2 & \\
- & 6X-6X^2 & \\ \hline
 & 12X^2 & \\
- & 12X^2-12X^3 & \\ \hline
 & 12X^3 &
\end{array}$$

On en déduit

$$\frac{X^4+1}{(X-1)^3(X-2)} = 1 - \frac{2}{(X-1)^3} - \frac{6}{(X-1)^2} - \frac{12}{X-1} + \frac{d}{X-2}.$$

Pour calculer $d$, on multiplie la fraction rationnelle par $X-2$, puis on prend la valeur en 2. On obtient $d = \dfrac{2^4+1}{(2-1)^3} = 17$, d'où la décomposition

$$\frac{X^4+1}{(X-1)^3(X-2)} = 1 - \frac{2}{(X-1)^3} - \frac{6}{(X-1)^2} - \frac{12}{X-1} + \frac{17}{X-2}.$$

## Exercices

1. Notons $\mathbb{Z}[i]$ l'ensemble des nombres complexes qui s'écrivent $a+bi$, où $a$ et $b$ appartiennent à $\mathbb{Z}$.

**a)** Montrer que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$.

**b)** Soit $z \in \mathbb{Z}[i]$. Montrer que $\bar{z} \in \mathbb{Z}[i]$ et que $|z|^2 \in \mathbb{N}$.

**c)** Soit $z \in \mathbb{Z}[i]$. Montrer que $z$ appartient au groupe des éléments inversibles de l'anneau $\mathbb{Z}[i]$ si et seulement si l'on a $|z|^2 = 1$.

**d)** Expliciter les éléments du groupe $(\mathbb{Z}[i])^*$.

2. Notons $\mathbb{Z}[\sqrt{2}]$ l'ensemble des nombres réels de la forme $a+b\sqrt{2}$, où $a,b \in \mathbb{Z}$. Nous avons montré dans l'exemple page 266 que $\mathbb{Z}[\sqrt{2}]$ est un sous-anneau de $\mathbb{R}$.

a) Montrer que $3+2\sqrt{2}$ est un élément inversible de l'anneau $\mathbb{Z}[\sqrt{2}]$ et calculer son inverse.

b) Montrer qu'il existe une infinité d'éléments inversibles dans l'anneau $\mathbb{Z}[\sqrt{2}]$.

3. Pour tout nombre premier $p$, notons $\mathbb{Q}(\sqrt{p})$ l'ensemble des nombres réels qui s'écrivent $a+b\sqrt{p}$, où $a$ et $b$ sont des nombres rationnels.

a) Soit $p$ un nombre premier. Montrer que $\mathbb{Q}(\sqrt{p})$ est un $\mathbb{Q}$-espace vectoriel de dimension 2.

b) Soit $p$ un nombre premier. Montrer que $\mathbb{Q}(\sqrt{p})$ est un sous-corps de $\mathbb{R}$.

c) Montrer que $\sqrt{2}$ n'appartient pas à $\mathbb{Q}(\sqrt{3})$.

d) Montrer que l'on a $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt{3}) = \mathbb{Q}$.

4. Posons $\alpha = \sqrt[3]{5}$ et notons $\mathbb{Q}(\alpha)$ l'ensemble des nombres réels qui s'écrivent $a+b\alpha+c\alpha^2$, où $a,b,c$ sont des nombres rationnels.

a) Montrer que $X^3-5$ est un polynôme irréductible de $\mathbb{Q}[X]$.

b) Soit $P$ un polynôme non nul de $\mathbb{Q}[X]$, de degré inférieur ou égal à 2. Montrer qu'il existe qu'il existe $U,V \in \mathbb{Q}[X]$ tels que $(X^3-5)U+PV=1$ et $\deg V \leqslant 2$. Calculer $P(\alpha)V(\alpha)$.

c) Montrer que $(1,\alpha,\alpha^2)$ est une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}(\alpha)$.

d) Montrer que $\mathbb{Q}(\alpha)$ est un sous-corps de $\mathbb{R}$.

5. Décomposer la fraction rationnelle $\dfrac{2X^3+1}{(X+1)(X^2-3X+2)}$ en éléments simples sur $\mathbb{R}$.

6. a) Factoriser le polynôme $X^4+X^2+1$ en produit de polynômes irréductibles de $\mathbb{R}[X]$.

b) Décomposer en éléments simples sur $\mathbb{R}$ la fraction rationnelle $\dfrac{2X}{X^4+X^2+1}$.

7. Notons $j$ une racine complexe du polynôme $X^2+X+1$.

a) Montrer que $(1,j)$ est une base de $\mathbb{C}$ sur $\mathbb{R}$. Calculer les coordonnées de $j^3$ et de $(j+1)^2$ dans cette base.

b) Décomposer la fraction rationnelle $\dfrac{X^4+1}{(X+1)^2(X^2+X+1)}$ en éléments simples sur $\mathbb{R}$.

8. a) Décomposer en éléments simples sur $\mathbb{R}$ la fraction rationnelle $\dfrac{X^2-1}{(X^2+1)^2}$.

b) Décomposer en éléments simples sur $\mathbb{C}$ la fraction rationnelle $\dfrac{X^2-1}{(X^2+1)^2}$.



9. Décomposer en éléments simples sur $\mathbb{R}$ la fraction rationnelle $\dfrac{X^2+1}{(X-1)^4(X-2)^2}$.

10. Soit $n$ un entier positif. Décomposer en éléments simples sur $\mathbb{R}$ la fraction rationnelle $\dfrac{1}{X(X+1)^n}$.

11. Existe-t-il une fraction rationnelle $F \in \mathbb{R}(X)$ telle que $F^2 = (X^2+1)^3$ ?

## Quelques réponses ou indications

1. c) Si $z$ est un élément inversible de l'anneau $\mathbb{Z}[i]$, alors par définition, il existe $z' \in \mathbb{Z}[i]$ tel que $zz'=1$. On a alors $|z|^2|z'|^2=1$. Utiliser la question (b) pour conclure.

d) On a $(\mathbb{Z}[i])^* = \{1,-1,i,-i\}$.

2. a) Chercher des entiers $a$ et $b$ tels que $(3+2\sqrt{2})(a+b\sqrt{2})=1$.

b) L'ensemble des éléments inversibles d'un anneau est un groupe pour l'opération produit, donc pour tout $n \in \mathbb{Z}$, le nombre $(3+2\sqrt{2})^n$ est un élément inversible de l'anneau $\mathbb{Z}[\sqrt{2}]$.

3. a) Les règles de calcul dans $\mathbb{R}$ font de $\mathbb{R}$ un espace vectoriel sur $\mathbb{Q}$, où la multiplication du scalaire $\lambda \in \mathbb{Q}$ par le vecteur $x \in \mathbb{R}$ est simplement le produit des deux nombres réels $\lambda$ et $x$. Par définition, $\mathbb{Q}(\sqrt{p})$ est le sous-espace vectoriel de $\mathbb{R}$ engendré par 1 et $\sqrt{p}$. Montrer que $(1,\sqrt{p})$ est une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}(\sqrt{p})$, en utilisant un résultat de la page 200.

c) Raisonner par l'absurde en supposant qu'il existe des nombres rationnels $a,b$ tels que $\sqrt{2}=a+b\sqrt{3}$. Élever au carré chaque membre de cette égalité et en déduire une contradiction.

d) Montrer que la dimension sur $\mathbb{Q}$ du sous-espace vectoriel $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt{3})$ de $\mathbb{Q}(\sqrt{2})$ est égale à $1$.

4. b) Les polynômes $X^3-5$ et $P$ sont premiers entre eux. D'après le théorème de Bézout, il existe des polynômes $U_0$ et $V_0$ tels que $(X^3-5)U_0+PV_0=1$. Écrire tous les polynômes $U,V$ solutions de l'équation $(X^3-5)U+PV=1$ en fonction de $U_0,V_0$ pour démontrer la première partie de la question.

c) Comme dans l'exercice précédent, $\mathbb{Q}(\alpha)$ est le sous-espace vectoriel du $\mathbb{Q}$-espace vectoriel $\mathbb{R}$, engendré par $1,\alpha,\alpha^2$. Utiliser (b) pour démontrer que $1,\alpha,\alpha^2$ sont linéairement indépendants.

d) Montrer tout d'abord que $\mathbb{Q}(\alpha)$ est un sous-anneau de $\mathbb{R}$. Utiliser ensuite (b).

5. On a $\dfrac{2X^3+1}{(X+1)(X^2-3X+2)} = 2 - \dfrac{1}{6(X+1)} - \dfrac{3}{2(X-1)} + \dfrac{17}{3(X-2)}$.

6. a) On a $X^4+X^2+1=(X^2+1)^2-X^2$.

7. b) Suivre la méthode de l'exemple 3 du cours. Pour trouver le numérateur de l'élément simple de dénominateur $X^2+X+1$, multiplier la fraction rationnelle par $X^2+X+1$, puis prendre la valeur en $j$.

8. a) Faire la division euclidienne de $X^2-1$ par $X^2+1$.

9. Conduire les calculs comme dans l'exemple 5. On trouve

$$\frac{X^2+1}{(X-1)^4(X-2)^2} = \frac{2}{(X-1)^4} + \frac{6}{(X-1)^3} + \frac{11}{(X-1)^2} + \frac{16}{X-1} + \frac{5}{(X-2)^2} - \frac{16}{X-2}.$$

10. Pratiquer la division selon les puissances croissantes comme dans l'exemple 5. On obtient

$$\frac{1}{X(X+1)^n} = \frac{1}{X} - \left(\frac{1}{X+1} + \frac{1}{(X+1)^2} + \cdots + \frac{1}{(X+1)^n}\right)$$

11. Raisonner comme dans l'application page 200.





# Quelques repères historiques

Voici quelques jalons permettant de situer, dans l'histoire des mathématiques, les principaux résultats du programme d'algèbre de première année. De l'œuvre des grands mathématiciens que nous allons citer, nous ne retenons que les travaux qui concernent directement ces résultats.

**L'arithmétique.** Dans les treize livres qui constituent les *Éléments* du mathématicien grec EUCLIDE, écrits au troisième siècle avant notre ère, se trouvent déjà exposées, de manière très rigoureuse, les propriétés arithmétiques élémentaires des nombres entiers positifs : divisibilité, proportionnalité, nombres premiers entre eux, existence et algorithme de calcul du plus grand commun diviseur, définition d'un nombre premier et démonstration qu'il existe une infinité de nombres premiers. Citons par exemple la première proposition du livre VII qui décrit la méthode à utiliser pour dire si deux entiers positifs sont premiers entre eux (c'est le procédé qu'on appelle maintenant algorithme d'Euclide) :

> *Deux nombres inégaux étant proposés, le plus petit étant de façon continue retranché du plus grand, si le reste ne mesure celui qui est avant lui que lorsqu'on a pris l'unité, les nombres proposés sont premiers entre eux.*

Au XVII[e] siècle, l'arithmétique connaît un nouvel essor avec PIERRE DE FERMAT (1601–1665). Celui-ci énonce que si $p$ est un nombre premier et si $a$ est un entier positif premier à $p$, alors l'entier $a^{p-1}-1$ est multiple de $p$ ; ce résultat, appelé « petit théorème de Fermat », ne sera démontré qu'en 1760 par LEONHARD EULER (1707–1783), sous une forme plus générale. FERMAT étudie aussi la célèbre équation $x^n + y^n = z^n$, où les inconnues $x$, $y$ et $z$ sont des nombres rationnels positifs : il affirme que cette équation n'a pas de solution si l'entier $n$ est supérieur ou égal à 3 et donne une ingénieuse démonstration pour l'équation $x^4 + y^4 = z^4$. Le cas $n = 3$ sera essentiellement traité par Euler et Gauss. L'affirmation de Fermat, appelée « grand théorème de Fermat », est devenue par la suite de plus en plus crédible ; elle a mobilisé les efforts de nombreux mathématiciens et a été un stimulant pour des avancées considérables dans plusieurs domaines des mathématiques ; ce n'est qu'en 1994 que le mathématicien anglais ANDREW WILES a pu démontrer un résultat très attendu dont on savait déjà qu'il impliquait le « grand théorème de Fermat ».

En 1801, le mathématicien allemand KARL-FRIEDRICH GAUSS (1777–1855) publie à 24 ans ses *Disquisitiones arithmeticæ*, un ouvrage qui fait de l'arithmétique une théorie à part entière. Dans les trois premières sections du traité, qui en compte sept, GAUSS définit la notion de congruence, en propose la notation $a \equiv b\ (n)$ et en fixe les règles de calcul. Il étudie ensuite l'équation $ax + b \equiv c\ (n)$ et utilise les congruences pour démontrer le petit théorème de Fermat.

**Les nombres complexes.** Dès que les mathématiciens ont voulu résoudre des équations polynomiales de degré au moins égal à 2, il devint nécessaire de considérer des racines carrées de nombres négatifs. Leur emploi soulève alors bien des réticences, parfois teintées de mysticisme. Ainsi GIROLAMO CARDANO (1501–1576), célèbre pour sa résolution des équations de degré 3, qualifie de « sophistiquées » les quantités $5 \pm \sqrt{-15}$ qu'il obtient en cherchant deux nombres $x$ et $y$ dont la somme est 10 et le produit 40. Si RAPHAEL BOMBELLI (vers 1526–1573) et GOTTFRIED WILHELM LEIBNIZ (1646–1716) précisent les règles de calcul sur les nombres complexes (appelés nombres imaginaires) et perçoivent l'opération de conjugaison, c'est CASPAR WESSEL (1745–1818) et ROBERT ARGAND (1768–1822) qui donnent aux nombres complexes leur représentation géométrique comme des points du plan. Il revient à GAUSS le mérite, non seulement de formuler clairement ce résultat et d'adopter la notation $a + bi$ (où $i^2 = -1$), mais aussi de découvrir de nombreuses applications des nombres complexes à l'arithmétique, l'analyse et la géométrie. Voici un extrait d'une lettre que GAUSS écrit en 1811 :

> *De même qu'on peut se représenter le domaine entier de toutes les quantités réelles au moyen d'une ligne droite indéfinie, de même on peut se figurer le domaine entier de toutes les quantités, les quantités réelles et imaginaires au moyen d'un plan indéfini où tout point, déterminé par son abscisse a et son ordonnée b, représente pour ainsi dire la quantité $a + bi$.*

**Les polynômes.** Dans l'œuvre du mathématicien grec DIOPHANTE (peut-être IIIe siècle), on trouve un système assez complet d'abréviations pour décrire les opérations (addition, soustraction, multiplication et élévation à une puissance entière) non seulement sur les nombres mais aussi sur des quantités numériques inconnues. DIOPHANTE sait résoudre diverses équations particulières du premier et du second degré, mais les symboles qu'il introduit par commodité ne font cependant pas eux-même l'objet d'opérations algébriques formelles.

L'aube du calcul algébrique se lève avec l'essor des mathématiques arabes, à partir du VIIe siècle. Le mot algèbre vient d'ailleurs de l'arabe al-jabr : ce terme désignait à peu près l'opération qui en langage moderne, consiste dans une égalité, à faire passer un terme d'un membre à l'autre en changeant son signe. Dans le livre de MUHAMMAD AL-KHWARIZMI (première moitié du IXe siècle), figure déjà une étude générale et détaillée des équations du second degré, bien que les seules racines reconnues pour ces équations soient celles qui sont positives et de préférence rationnelles. Un pas supplémentaire est franchi avec AL-KARAGI (fin du Xe, début du XIe siècle) qui initie le calcul sur les puissances entières positives ou négatives de l'inconnue ($x^p x^q = x^{p+q}$, $x^p / x^q = x^{p-q}$) et démontre de nombreuses identités algébriques. Au début du XIIe siècle, AL-SAMAW'AL est en possession du calcul algébrique général sur les expressions polynomiales, y compris la division euclidienne.

Par la suite, de nombreux mathématiciens s'efforceront de trouver des expressions pour les racines d'équations algébriques, souvent au moyen de méthodes très astucieuses. Peu à peu s'établit la conviction qu'une équation polynomiale de degré $n \geqslant 1$ possède toujours exactement $n$ racines, éventuellement complexes, à condition de compter chacune d'elles avec son ordre de multiplicité. Pour comprendre l'importance théorique de cette affirmation, qu'on appelle maintenant le théorème fondamental de l'algèbre, il faut savoir que les tentatives de calcul des racines en utilisant des radicaux se soldent par des échecs, sauf dans le cas des équations de degré inférieur ou égal à 4 ou d'équations bien particulières. C'est GAUSS qui trouve la première démonstration de ce théorème en 1799. Il publiera ensuite trois autres démonstrations, la dernière étant relative à des polynômes dont les coefficients sont des nombres complexes. Depuis le profond travail d'ÉVARISTE GALOIS (1811–1832), on sait qu'il n'est en général pas possible d'exprimer par des radicaux les racines d'un polynôme de degré au moins égal à 5.

**L'algèbre linéaire.** Bien que l'on trouve trace dans un ancien traité chinois d'une technique pour résoudre certains systèmes de trois équations linéaires à trois inconnues, la théorie des équations linéaires est relativement récente : elle ne s'établit en effet qu'au XVIIIe siècle avec le calcul des déterminants et les formules de résolution de GABRIEL CRAMER (1704–1752). Peu après apparaît la possibilité de calculer un déterminant en le développant selon une ligne ou une colonne et GAUSS, qui adopte la disposition en tableau, donne la règle pour multiplier deux déterminants. La notion de matrice, dès lors présente en filigrane, est mise en évidence par JOSEPH SILVESTER (1814–1887) et ARTHUR CAYLEY (1821–1895) comme un outil de calcul très commode et CAYLEY établit les règles d'addition, de produit et de calcul de l'inverse d'une matrice.

C'est GÜNTHER GRASSMANN (1809–1877) qui dégage la notion de vecteur à $n$ coordonnées, précise les règles de calcul dans un espace vectoriel et introduit les notions de sous-espace vectoriel, de base et de dimension.

**Les structures algébriques.** La notion de structure algébrique, c'est-à-dire la mise en évidence et la formalisation de règles de calcul communes à diverses situations mathématiques apparemment étrangères les unes aux autres, n'apparaît pas avant le XIXe siècle.

En ce qui concerne la notion de groupe, c'est dans le cadre de son œuvre fondamentale sur la résolubilité par radicaux des équations algébriques, qu'ÉVARISTE GALOIS introduit le concept de groupe de permutation et surtout de sous-groupe du groupe symétrique. La définition abstraite d'un groupe (fini) est formulée en 1854 par CAYLEY qui perçoit dans cette structure la possibilité d'unifier de nombreux types de calcul : permutations, racines de l'unité, transformations géométriques et matrices inversibles, pour s'en tenir aux exemples les plus élémentaires. La définition d'un sous-groupe, d'un homomorphisme et bien d'autres notions générales sont bientôt introduites et étudiées en détail, notamment par CAMILLE JORDAN (1838–1922).

Dans la seconde moitié du XIX[e] siècle, les recherches en algèbre s'orientent progressivement vers l'étude des structures : celle d'anneau, avec ERNST KUMMER et RICHARD DEDEKIND qui généralisent les travaux arithmétiques de GAUSS, et celle de corps avec la construction par LEOPOLD KRONECKER de nouveaux corps de nombres (un corps de nombres est un sous-corps de $\mathbb{C}$ qui est de dimension finie en tant que $\mathbb{Q}$-espace vectoriel).

Au XX[e] siècle, la notion de groupe sera reconnue comme fondamentale dans tous les domaines des mathématiques, y compris en analyse et en géométrie. Plus généralement, les structures algébriques seront non seulement étudiées pour elles-mêmes, mais aussi largement utilisées dans toutes les branches des mathématiques.



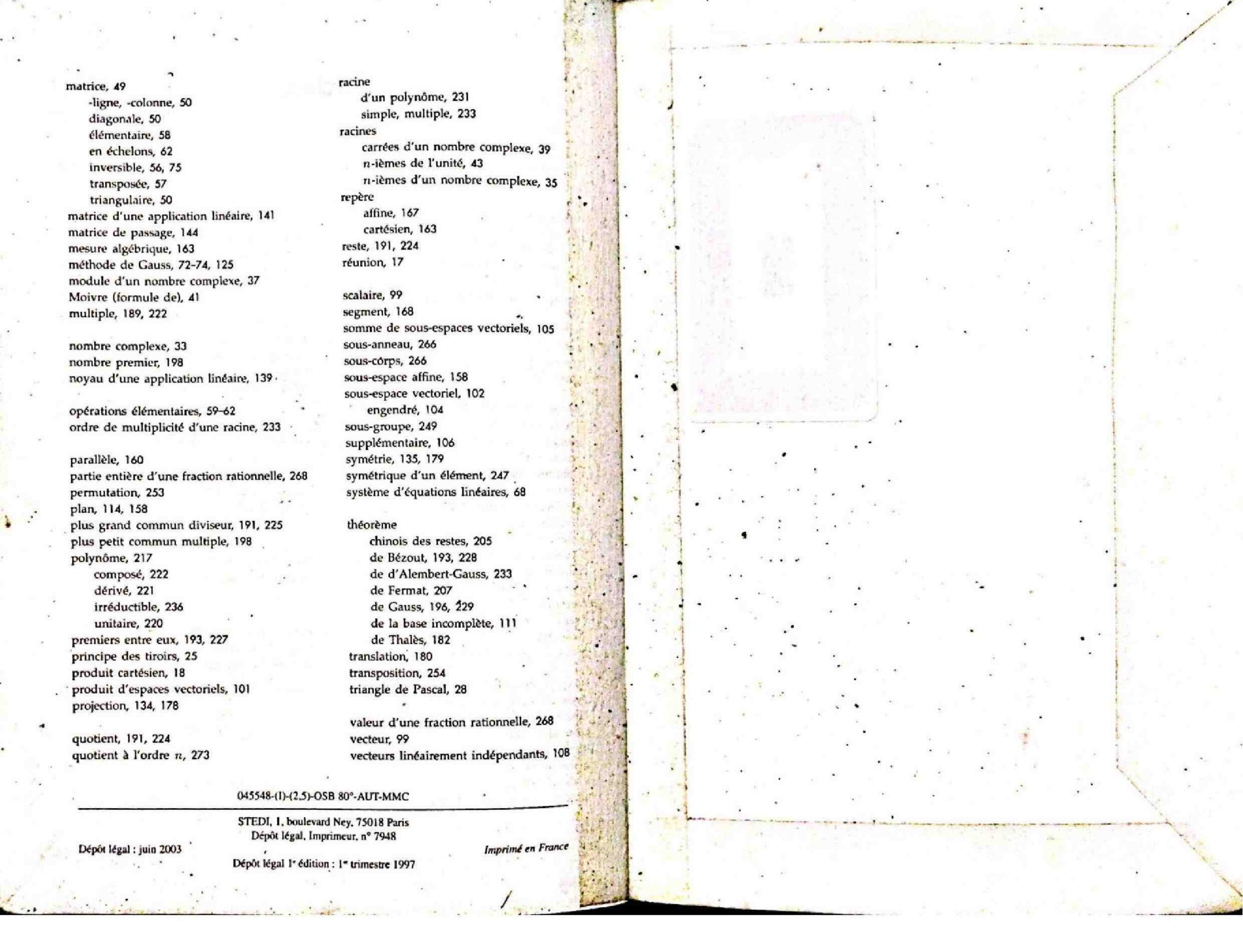


# Index





sigmakutub.blogspot.com

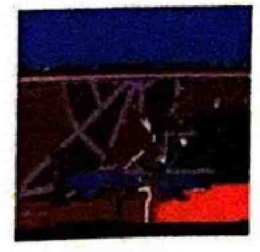




045548-(I)-(2,5)-OSB 80°-AUT-MMC

STEDI, 1, boulevard Ney, 75018 Paris
Dépôt légal, Imprimeur, n° 7948
Dépôt légal : juin 2003
Imprimé en France
Dépôt légal 1re édition : 1er trimestre 1997

SCIENCES SUP



*2e édition*

François Liret
Dominique Martinais

# ALGÈBRE
# 1re ANNÉE



Dans ce volume d'algèbre pour la première année, une partie importante est consacrée à l'algèbre linéaire : espaces vectoriels, bases, applications linéaires et calcul matriciel. L'arithmétique élémentaire et les polynômes font chacun l'objet d'un chapitre conséquent.

Le cours, entièrement révisé et complété dans cette nouvelle édition, présente les résultats essentiels et les énoncés les plus utiles. Il est illustré par des exemples détaillés et des exercices corrigés. Chaque chapitre se termine par de nombreux énoncés d'exercices suivis de brèves réponses ou d'indications. Certains sont un entraînement au calcul et d'autres sont rédigés en plusieurs questions permettant d'apprendre à raisonner.

FRANÇOIS LIRET
est maître de conférences à l'université Paris 7–Denis Diderot.

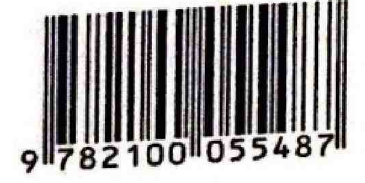
DOMINIQUE MARTINAIS
était maître de conférences à l'université Paris 7–Denis Diderot.

## COURS DE MATHÉMATIQUES

Ce cours de mathématiques traite en quatre volumes le programme des deux premières années des filières MIAS, MASS et SM.

- Analyse 1re année
- Algèbre 1re année
- Analyse 2e année
- Algèbre et géométrie 2e année

MATHÉMATIQUES
PHYSIQUE
CHIMIE
SCIENCES DE L'INGÉNIEUR
INFORMATIQUE
SCIENCES DE LA VIE
SCIENCES DE LA TERRE




ISBN 2 10 005548 8

http://www.dunod.com

